Quantum internet

The internet's next big step

Vermaas, Pieter; Nas, Deborah; Vandersypen, Lieven; Elkouss Coronas, David

Publication date
2019

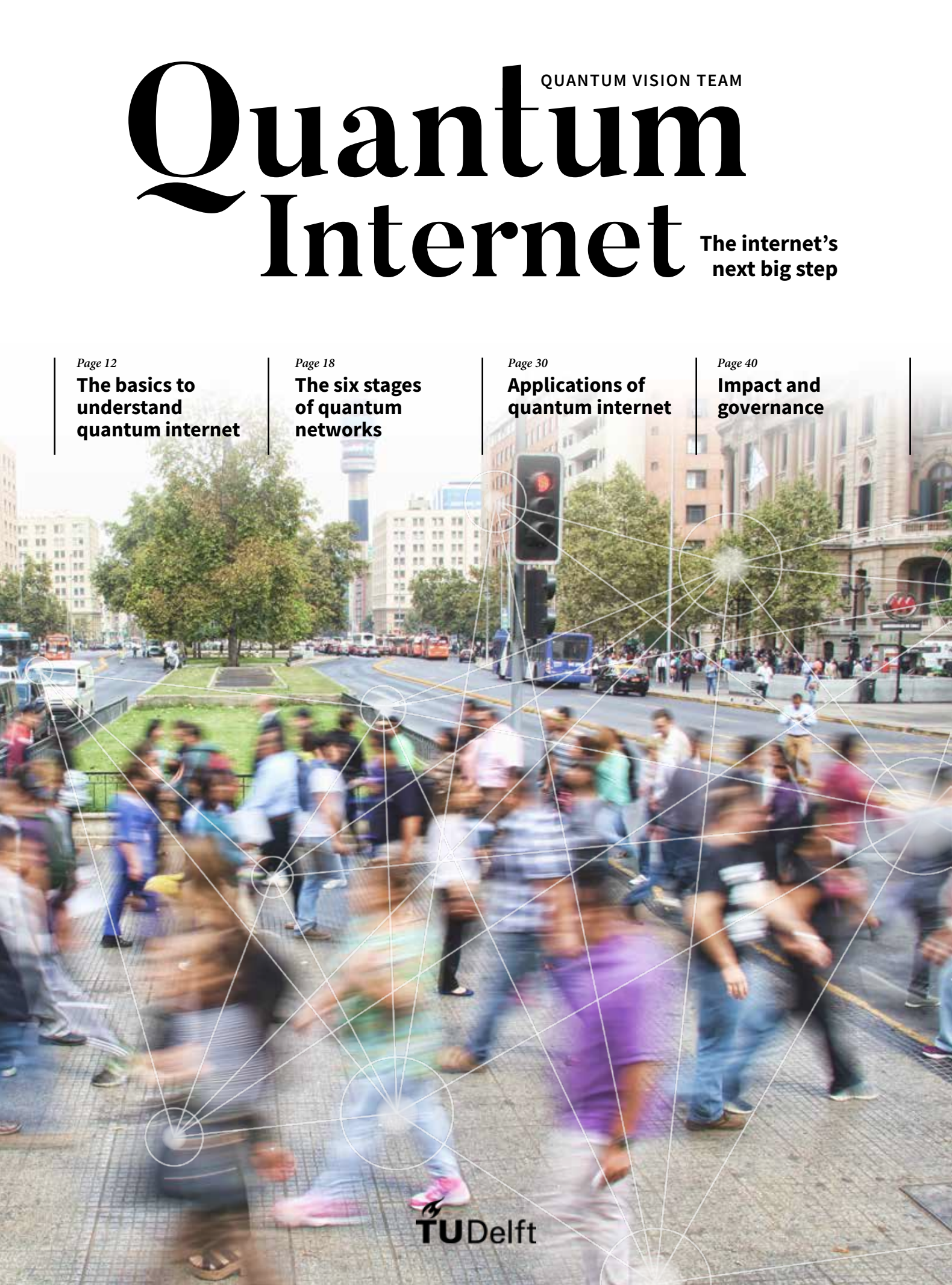
Document Version
Final published version

Citation (APA)
Vermaas, P., Nas, D., Vandersypen, L., & Elkouss Coronas, D. (2019). *Quantum internet: The internet's next big step*. Delft University of Technology. https://qutech.nl/quantum-internet-magazine/

QUANTUM VISION TEAM

Quantum Internet

The internet's next big step



TU Delft

The quantum vision team

Colophon

Production
The quantum vision team
Pieter Vermaas
Deborah Nas
Lieven Vandersypen
David Elkouss Coronas

Text and Editing
The quantum vision team
Aletta Meinsma
Agaath Diemel

Design
Júlia Fort Muñoz

Traffic Management
Media Solutions, TU Delft

Cover picture
Mauro Mora

Print
Edauw+Johannissen

'Quantum Internet: The internet's next big step' is a publication of the TU Delft

Quantum is coming. Based on research successes at TU Delft and elsewhere in the world, we confidently predict that quantum technology will increasingly lead to valuable applications in the next decades. Besides researching and developing quantum technology, TU Delft sees it as its responsibility to also investigate the consequences of such a new and ground-breaking technology. How will quantum technology impact industry and society at large? To some extent, this remains informed guesswork; as with all groundbreaking technology, its true impact will only become clear once it is out there.

There are some certainties, though. One of them is that quantum internet is a technology that is close to realisation; it is also a quantum technology that we work on at TU Delft. That is why in mid-2018 we formed a team, of scientists and engineers from all over the university, that set about exploring the consequences of having quantum internet. We studied national and international reports on quantum technologies, and spoke to people and organisations that are also involved in identifying societal issues that can emerge with the introduction of quantum internet. We organised workshops with science journalists, innovators and designers, industry, law enforcement and defence, and governmental organisations to discuss how quantum internet may impact society by changing communication and its security.

In this magazine we present the outcomes from our first exploration. It serves as a basis for further research on the societal impact of quantum technologies, at TU Delft and beyond, together with the scientists and engineers working on developing these promising new technologies. By creating a magazine, we hope to offer something to all, regardless of their knowledge level on quantum technology. For some, this magazine can help to gain a better understanding of how quantum internet and other quantum applications will work, for others it might be an incentive to join forces with TU Delft. We envision a future where all can benefit from the new applications that quantum technology can bring.

Pieter Vermaas (chair)
Deborah Nas
Lieven Vandersypen
David Elkouss Coronas

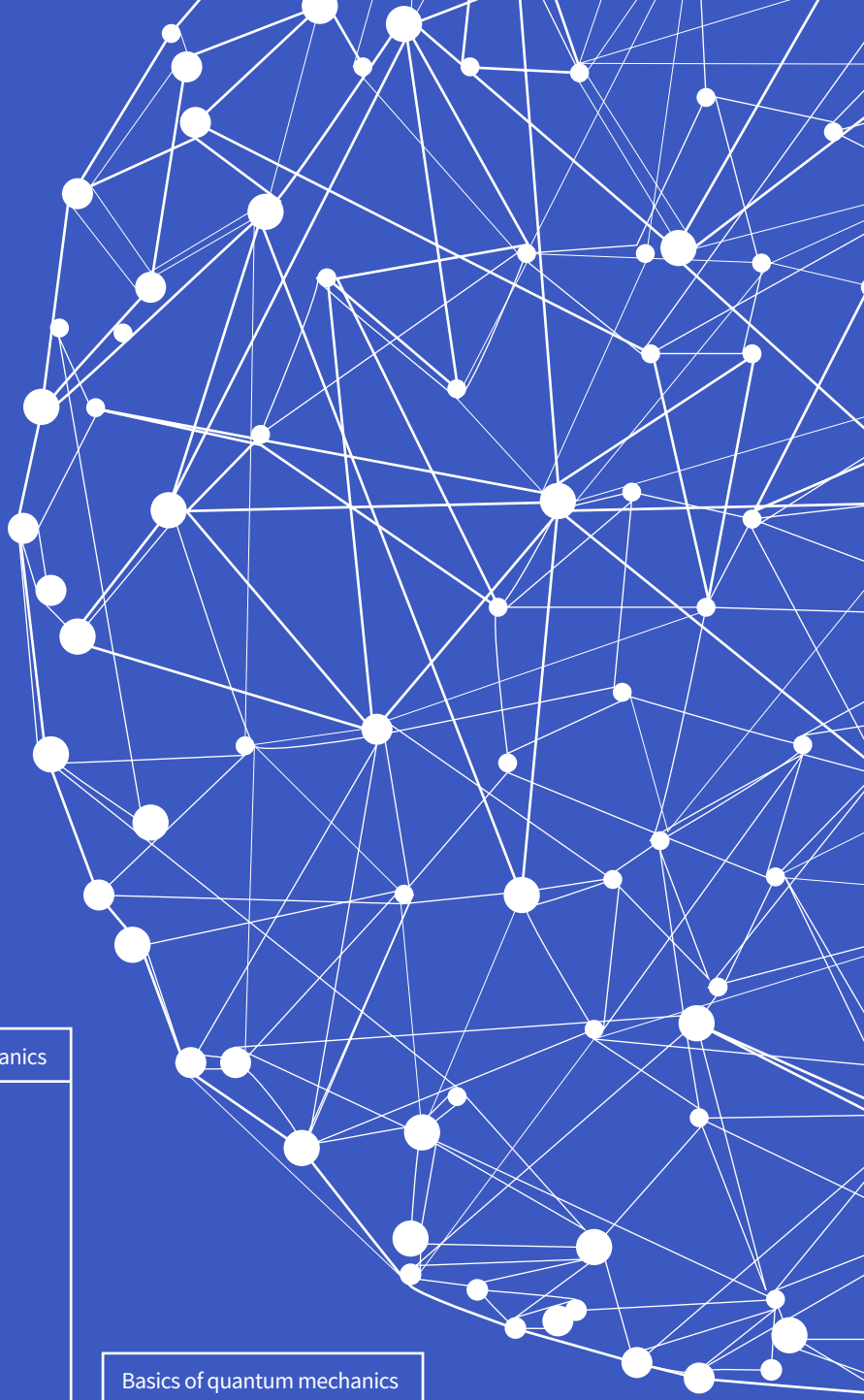
Lotte Asveld
Julia Cramer
Slava Dobrovitski
Willem Evers
Júlia Fort Muñoz
Marijn Janssen
Aletta Meinsma
Gary Steele
Tim Taminiau
Richard Versluis
Kees Vuik

Ronald Hanson
Scientific Director QuTech

QuTech is the research center for quantum computing and quantum internet, a collaboration founded in 2014 by TU Delft and the Netherlands Organisation for Applied Scientific Research (TNO). QuTech addresses scientific and engineering challenges, often together with industrial partners. QuTech is organized along roadmaps, and our work in the Roadmap Quantum Internet and Networked Computing, led by Stephanie Wehner, is currently creating the first tangible results. We build towards a first quantum internet in the Netherlands and we coordinate the European Quantum Internet Alliance. Therefore, this magazine focusses for good reason on the societal impact of quantum internet.

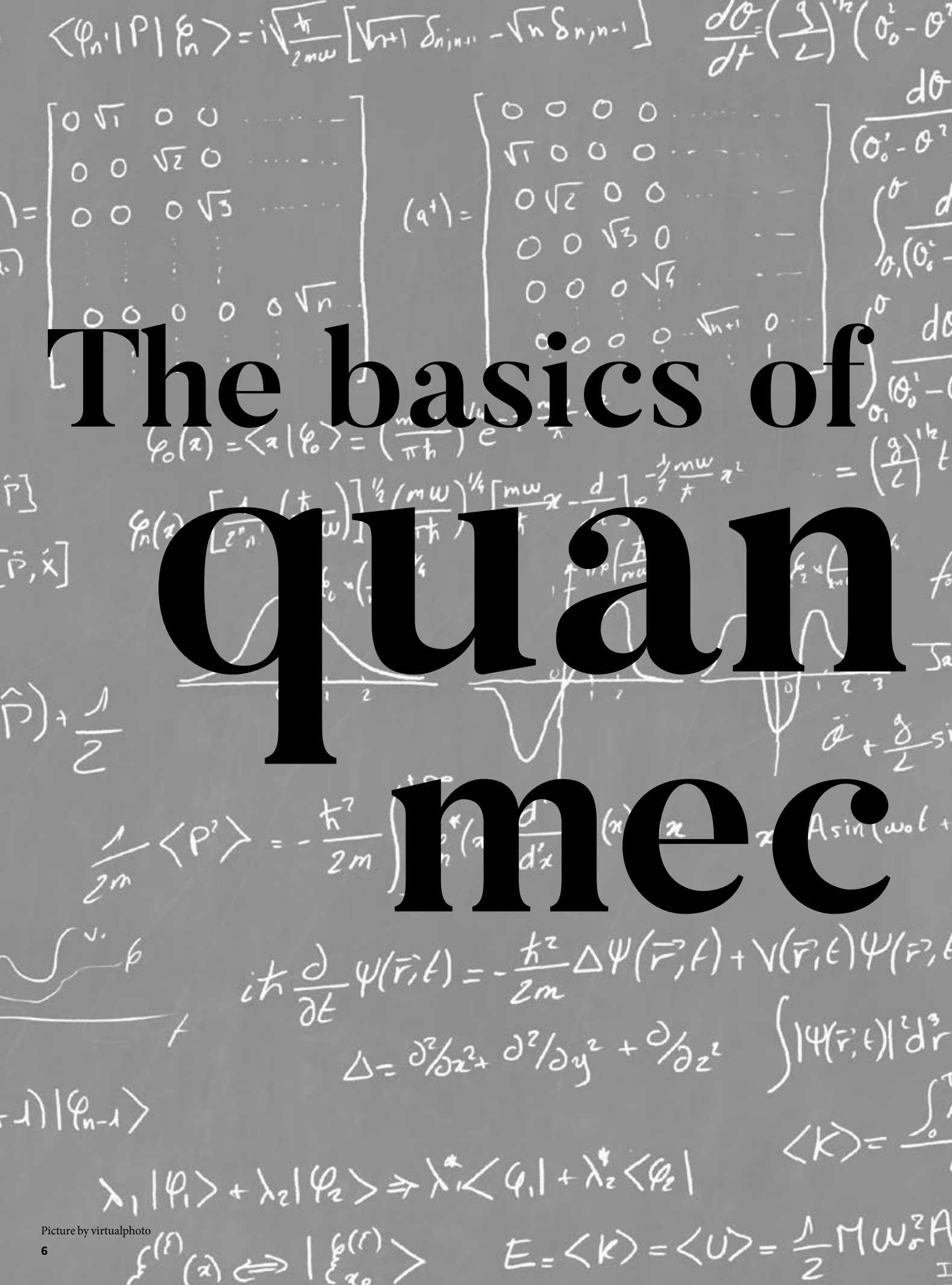
Tim van der Hagen
Rector Magnificus/President Executive Board Delft University of Technology

TU Delft has taken scientific and technological leadership in developing quantum technologies. Research at QuTech and at the Faculties of Applied Sciences and of Electrical Engineering, Mathematics & Computer Science is bringing quantum internet and quantum computation closer to realisation. TU Delft has decided that it should also take up its societal responsibility and for this the Executive Board launched in 2018 an effort to explore what impact quantum technologies can have on society and industry. This magazine is the result of this effort, focussing on the impact of quantum internet.

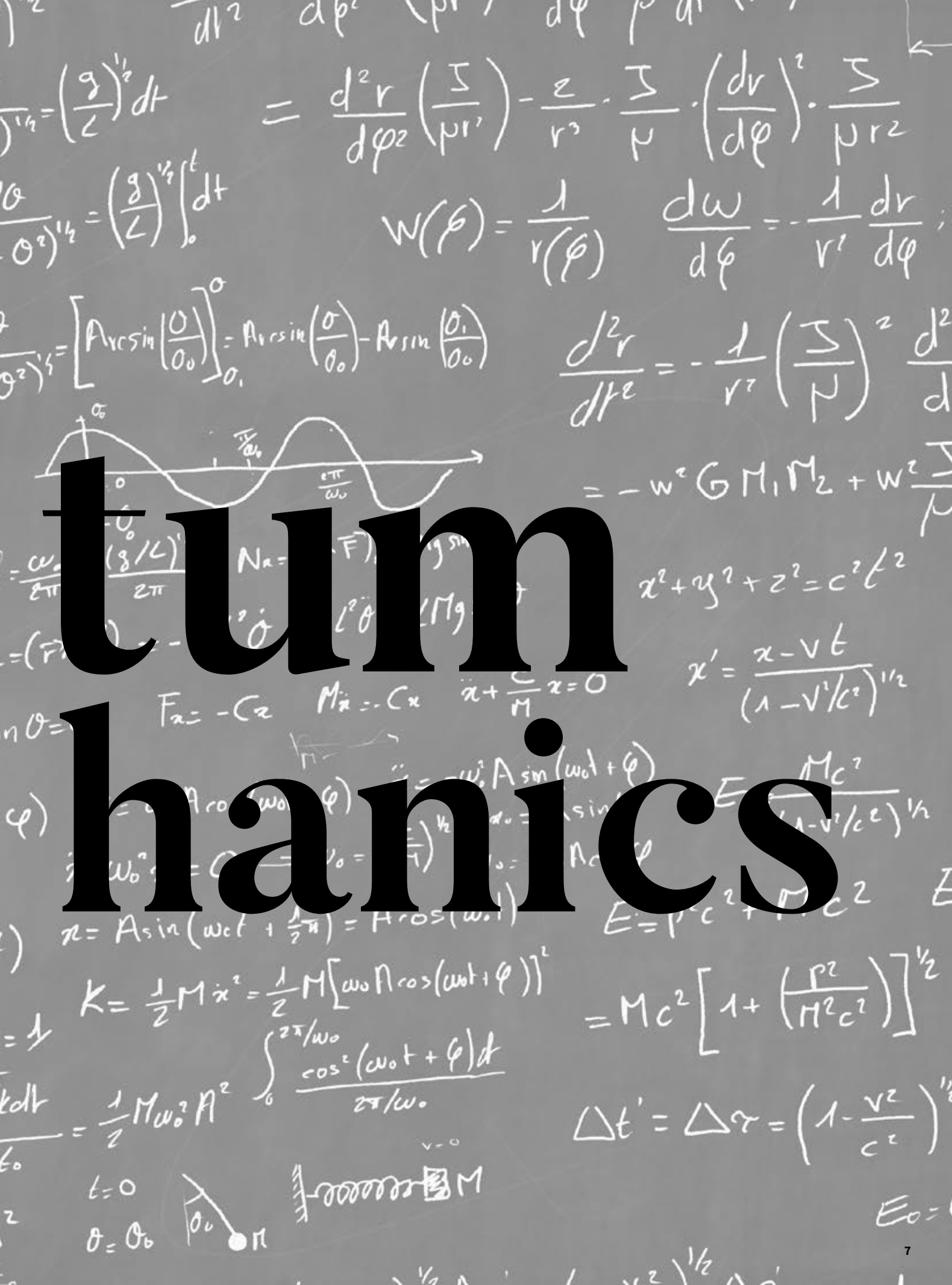


Contents

The basics of quan mec



Picture by virtualphoto



tum hanics

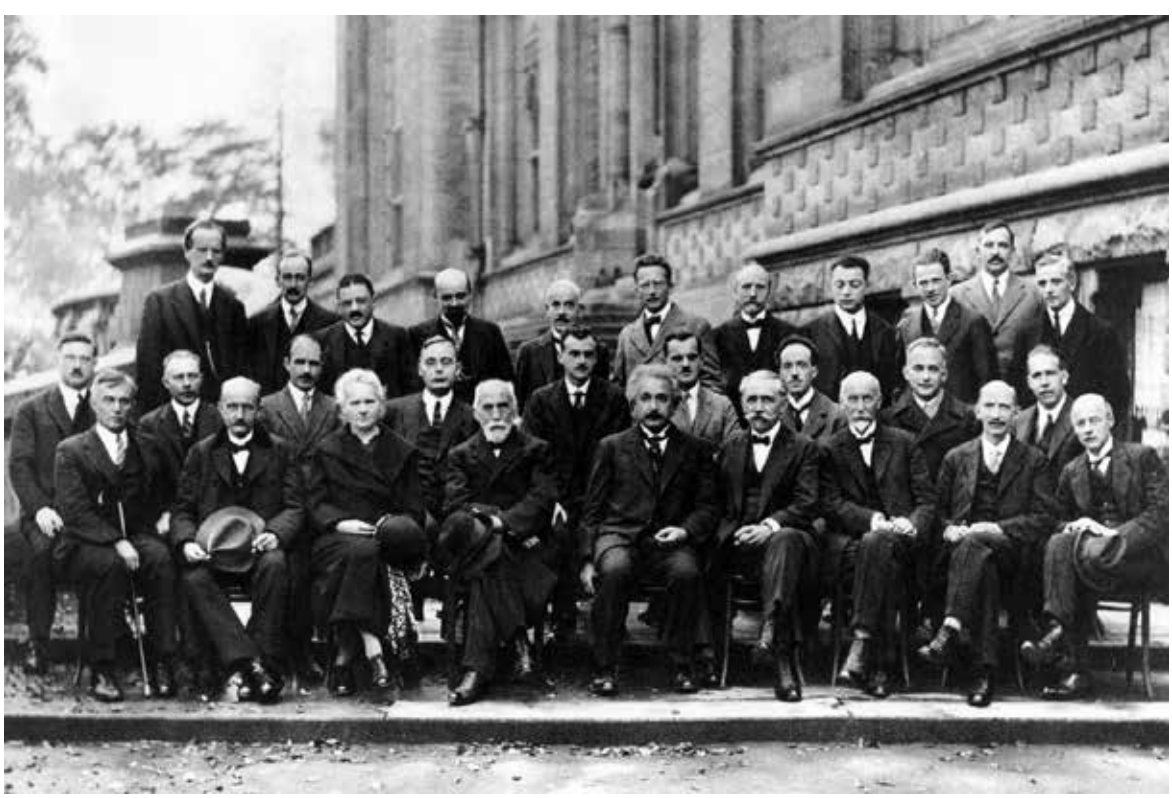
Quantum mechanics

and quantum technology 1.0

Quantum mechanics is the science of the very small. It explains the behavior of matter and its interactions with energy on the scale of atoms and subatomic particles.

Our understanding of quantum mechanics accelerated in the beginning of the 20th century. At the Solvay International Conference on Electrons and Photons, organised in 1927 in Brussels, 29 prominent physicists discussed the basics of quantum theory and laid the foundation for today's quantum mechanics. Seventeen of them already were, or would become, Nobel Prize winners. Amongst them were Albert Einstein, Marie Curie, Max Planck, and Niels Bohr.

Many technologies we use in modern life could be invented because of our understanding of quantum mechanics: lasers, MRI scanners, nuclear energy and transistors, to name a few. Quantum mechanics helped us to understand and manipulate semiconductors, the key enabler for the transistor, meaning that computers, tablets and smartphones all exist because we know how to make use of the effects of quantum mechanics.

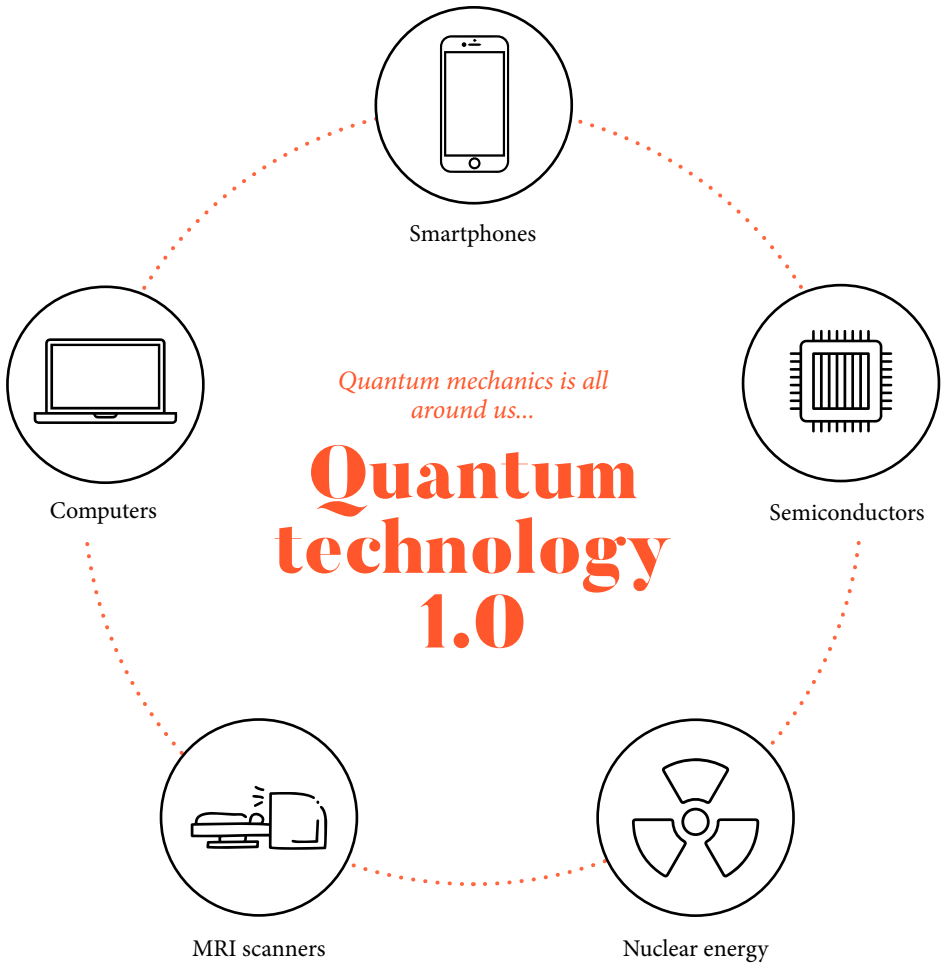


The Solvay Conference in 1927 in Brussels, 5th council of physics.

Back row L-R:
A. Piccard, E. Henriot, P. Ehrenfest, E. Herzen, Th. de Donder, E. Schrödinger, E. Verschaffelt, W. Pauli, W. Heisenberg, R. Fowler, L. Brillouin

Middle row L-R:
P. Debye, M. Knudsen, W.L. Bragg, H.A. Kramers. P.A.M Dirac, A. Compton, L. de Broglie, M. Born, N. Bohr

Front row L-R:
I. Langmuir, M. Planck, M. Curie, H. Lorentz, A. Einstein, P. Langevin, C. E. Guye, C.T.R Wilson, O.W. Richardson



Quantum mechanics is all around us...

Quantum technology 1.0

The kilogram

From May 2019, the definition of the kilogram is described by the laws of quantum mechanics.

Interested to learn more about the Planck constant?

Standards have undergone much-needed change throughout the last two centuries. Almost all standards in the International System of Units have now been redefined on the basis of physical constants rather than physical prototypes. The kilogram is the last unit of measure to be given a complete makeover. After almost 130 years, the definition of the kilo was changed. Up to May 2019, the unit was still based on a platinum-iridium alloy cylinder prototype created in 1889, which is kept in a vault in Paris and of which several replicas exist around the world.

The new definition is based on the Planck constant, an important constant in quantum mechanics. This way, the definition of a kilogram is more accurate than basing it on a physical object. Also, there will no longer be special institutes that own the truth about the kilogram. It will be owned by everyone, described in a formula.

2019

The kilogram is defined using the Planck constant (h)

$h = 6.62607004 \times 10^{-34}\ m^2\ kg\ /\ s$

1889

The kilogram was defined as being equal to the mass of the international prototype of the kilogram.

This gilded brass kilogram originates from the beginning of the 20th century and comes from the inventory of the Commission for the Supervision of Standards.

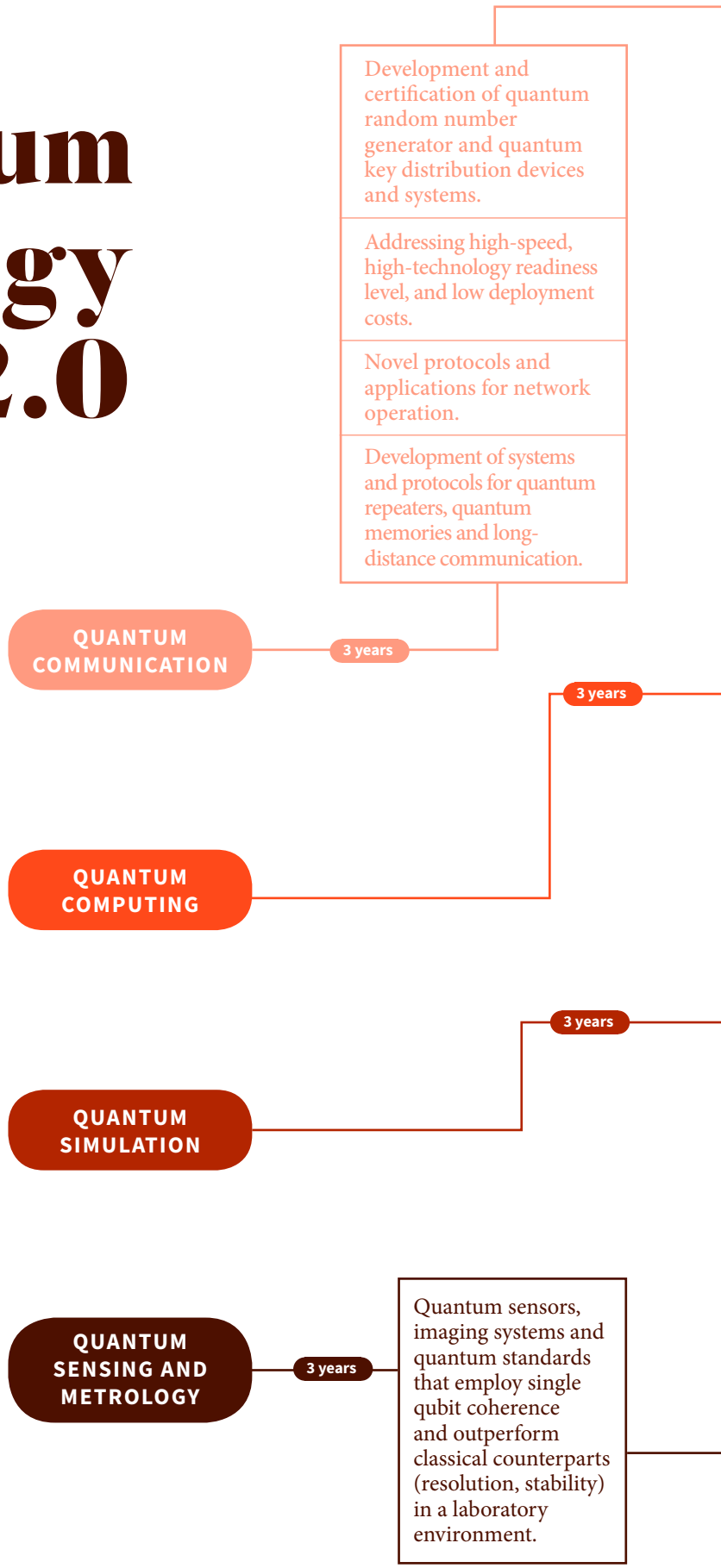
TU Delft Library / Special Collections.

1kg

Quantum technology 2.0

We are entering an era that we like to refer to as quantum 2.0. Not only are we able to understand the effects of quantum mechanics, we are now also able to actively manipulate individual particles at a quantum level and read out their states in a single shot. This allows us to develop quantum technologies that will enable new applications, spark many new businesses, and may help us solve some of the world's challenges.

To keep Europe at the forefront of the second quantum revolution now unfolding worldwide, the European Commission announced the Quantum Technology Flagship in 2016. They appointed an independent High-Level Steering Committee to deliver a Strategic Research Agenda, an Implementation model and a Governance model for each of the four quantum technologies: quantum communication, quantum computation, quantum simulation and quantum sensing and metrology.



Quantum technology 2.0 timeline

This roadmap cites the key milestones as published in the Quantum Technologies Flagship Final Report, published by the High-Level Steering Committee 28 June 2017.

6 years

- Cost-effective and scalable devices and systems for intercity and intra-city networks that demonstrate end-user-inspired applications.
- Scalable solutions for quantum networks that connect devices and systems, e.g. quantum sensors or processors.

10 years

- Development of autonomous metro-area, long distance (>1000 km) and entanglement-based networks, a 'quantum internet'.
- Protocols that exploit the novel properties that quantum communication offers.

6 years

- Fault tolerant routes for making quantum processors with eventually more than 50 qubits.

6 years

- Quantum processors fitted with quantum error correction or robust qubits that outperform physical qubits.

10 years

- Quantum algorithms that demonstrate quantum speed-up and outperform classical computers.

6 years

- Experimental devices with certified quantum advantage on the scale of more than 50 (processors) or 500 (lattices) individual coupled quantum systems.

6 years

- Quantum advantage in solving important problems in science (e.g. quantum magnetism).
- Quantum optimization (e.g. via quantum annealing).

10 years

- Prototype quantum simulators that solve problems beyond supercomputer capability, including in quantum chemistry, in the design of new materials, and in optimizing problems such as occurring within the context of artificial intelligence.

6 years

- Integrated quantum sensors, imaging systems and metrology standards at the prototype level, with first commercial products brought to the market.
- Laboratory demonstrations of entanglement enhanced technologies in sensing.

10 years

- Transition from prototypes to commercially available devices.

The basics to understand

Quantum internet

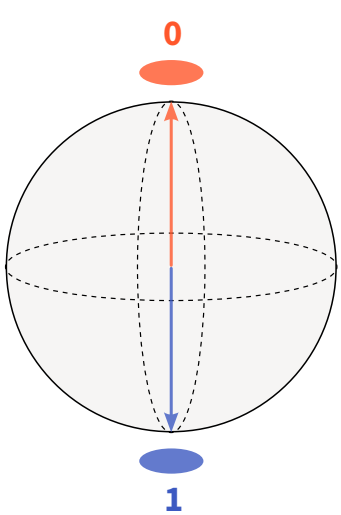
In our everyday lives we experience the world according to the rules of classical physics. However, at much smaller scales, the scales of atoms and electrons, we enter a world where different rules apply: the rules of quantum mechanics.
Since we don't experience this in our everyday lives, it's really hard to imagine quantum mechanics. To understand the working of a quantum internet, you have to understand the three ways in which quantum mechanics, at its core, differs from classical physics. These three concepts are quantum superposition, measurement and entanglement.

Picture by Christian Zachariasen

It's like a spinning coin, if you look from above it's heads and tails at the same time.

Qubits

Before diving into the three concepts of quantum mechanics, it's important to know that the building blocks of a quantum internet are quantum bits, or qubits. Qubits can be compared to classical bits, except that qubits work with these three concepts of quantum mechanics. We represent a qubit as a sphere that has value 0 on the north pole and value 1 on the south pole. While a classical bit can only take value 0 or value 1, a qubit can have any value on this sphere. This brings us to the concept of superposition: a qubit can take the value of 0 and 1 at the same time!



Superposition

The first concept is quantum superposition: in quantum mechanics, objects are allowed to be in two places at the same time. This is a strange concept, but the fact that things can be in two places at the same time is something that you just have to accept: if it were not true, every atom in every object on the earth would collapse into itself on a time scale of a few picoseconds. The fact that the matter we are made of is stable, was one of the most spectacular predictions of quantum mechanics.
We don't experience super-position in our daily life: for us, an object is never in two places at the same time. To get a feeling of what superposition means, imagine spinning a coin on its side. If you look from above to the spinning coin, you can see both sides of the coin: it is like the coin is both heads as well as tails in that specific moment in time, just like a qubit can be in two states at the same time.

Measurement

The second strange thing about quantum mechanics is what happens when you look: in classical mechanics, looking at something does not change the 'state' of that thing. If you look at a car driving down the road, the car is still driving down the road after you have looked at it. This, it turns out, is different in quantum mechanics. If you look at a quantum superposition of an object – the object is in two places at the same time – the object itself will 'jump' to one position or the other. The fact that you have acquired knowledge about the object has changed its state. In the analogy of the spinning coin, you can compare this looking at the coin to slapping the spinning coin on the table: the coin is forced to choose a side. This second 'strange' property of quantum mechanics has been confirmed by decades of experiments.

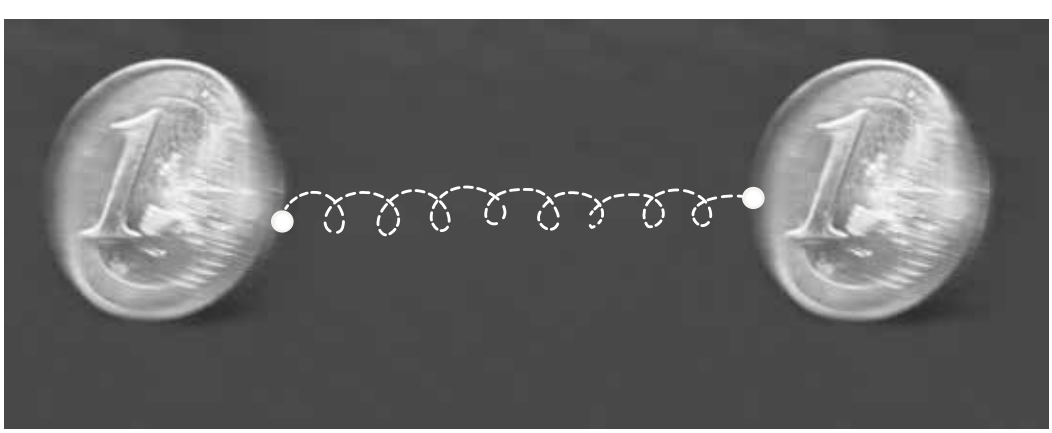
Keeping your information is a difficult task

Maintaining the superposition state of a qubit is quite a challenging task and one of the difficulties in building a quantum internet. Physical qubits decohere after some time, meaning the qubit isn't in superposition anymore, but takes on a value of 0 or 1. In the analogy of the spinning coin this means that after some time, the coin loses speed and falls over to one side. The coin obtains either the value 'heads' or the value 'tails'.

Entanglement

The third concept is that of entanglement: two qubits can have an extremely strong connection. If two qubits are entangled, and both qubits are measured, the outcome for each qubit will look random. But, once you compare the outcomes, you find that they match up in ways that are simply impossible to achieve with classical bits. The outcomes can only be explained if the measurement on one qubit has somehow influenced the other qubit.
This entanglement remains in existence when the two qubits are sent far apart. Say, one qubit is sent from Delft to New York, and the other from Delft to Tokyo. A measurement then taken on the New York qubit immediately influences the Tokyo qubit. Returning to the analogy, entanglement of two spinning coins means that if you repeatedly spin and slap both coins on the table, you will find 'heads' and 'tails' in combinations that are impossible, unless the coins have immediate interaction with each other, even while one is in New York and the other in Tokyo.

Einstein referred to entanglement of qubits as 'spooky action at a distance'. It may be spooky from the perspective of our daily lives, yet on the scale of atoms and electrons it is a regular phenomenon.



...they have an extremely strong connection.

Why do we actually want to build a quantum internet?

Apart from the fact that the process teaches us new physics, will a quantum internet have added value over the classical internet - the internet that we are currently all using? What are the differences and similarities between the classical and quantum internet?

WHAT IS IT?

Classical internet

If you send digital information over the classical internet, this information is built up of bits. A bit can take two values: we call them 0 or 1.

For example, we can send the following digital information from our computer to another computer by using the classical internet:

01001001
01101110
01110100
01100101
01110010
01101110
01100101
01110100

And while for us this looks like a random bunch of 0 and 1's, a computer knows that, in a kind of encoding called ASCII, we've actually sent over a word - namely the word 'Internet'.

Development

During the cold war, the US military feared that a Soviet attack could easily destroy the whole telephone network. If that would happen, long-distance communication would not be possible anymore. A scientist working for the Massachusetts Institute of Technology (MIT) as well as the U.S. Defense's Advanced Research Projects Agency (DARPA) consequently developed a network between computers. This ARPANET would be less vulnerable to a Soviet attack than the telephone network. By connecting computers with cables, information could be sent from computer to computer. Furthermore, a method was developed that was able to break down information into smaller packets, so that each packet could take its own route between the computers. The very first attempt to send a message over the ARPANET – the word "LOGIN" – was undertaken in 1969.

"LOGIN"

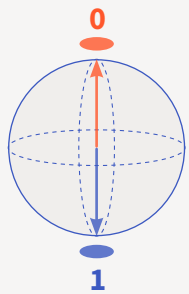
At the University of California at Los Angeles (UCLA), they typed an "L". And in Stanford University an "L" appeared on the screen. Afterwards at UCLA the letter "O" was sent. In Stanford, they could now see "LO" on the screen. The third letter, "G", crashed the system.

WHAT IS IT?

Quantum internet

A quantum internet works with quantum bits – so called qubits. Qubits follow the rules of quantum mechanics.

Qubits cannot be measured without being disturbed. This is a big advantage for the security of the quantum internet, but at the same time forms a difficulty for communicating over larger distances because it makes it impossible to amplify or repeat the signal.



PAGES 12 and 13.
More information on qubits and their properties.

PAGE 17.
More information on the security of a quantum internet.

PAGES 18 to 21.
More information on the six stages of quantum networks.

Development

One of the goals of QuTech is to develop the technology to enable quantum communication between any two places on earth. The first step towards achieving this goal is building the first real quantum network between the cities of Delft, The Hague, Leiden and Amsterdam. This quantum network should be up and running in 2022 and can be seen as the quantum version of the ARPANET.

Once a quantum network is operational in the Netherlands, the next step is to extend it to Europe. The European Quantum Internet Alliance, an alliance of Europe's quantum research institutes and actors from industry, works on a scalable design to make such a large-scale network possible.

Public key cryptography

Three decades after the first message had been sent over the ARPANET, the US National Institute of Standards and Technology (NIST) established an encryption standard called Advanced Encryption Standard (AES). This encryption standard (a type of symmetric encryption) is still used today, although much communication is currently secured via public key cryptography (asymmetric encryption).

CRYPTOGRAPHY

Classical post-quantum cryptography

Classical post-quantum cryptography, also referred to as quantum-proof or quantum-resistant cryptography, are techniques that are expected to be secure against attacks from quantum computers. One possible solution might be to use symmetric keys. Although a quantum computer running Grover's algorithm can break such a symmetric key, increasing the key size is expected to make it quantum-resistant. Other examples of public key cryptosystems that are believed to be secure against quantum computers are lattice-based cryptography, hash-based cryptography, code-based cryptography, multi-variate cryptography and supersingular isogeny-based cryptography. Some organisations are already implementing these cryptosystems, even though standards for classical post-quantum cryptography have not been agreed yet.

Classical internet

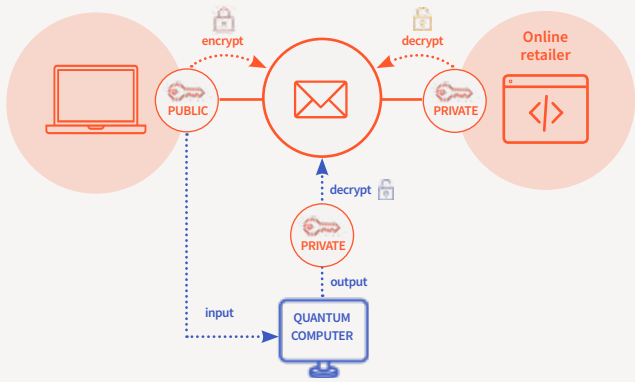
How does public key cryptography work?

If you buy something online, your communication with the online retailer is usually secured through public key cryptography. Public key cryptography works with a private key and a publicly available and freely shared key. You encode your message using the online retailer's public key and the online retailer decrypts the message with their private key.

Safety

If the message happens to be intercepted along the way by an eavesdropper, it is extremely difficult for that person to decode the information in your message. Only if the eavesdropper can get their hands on the private key, they can break the encryption. In some cases, the eavesdropper can obtain the private key from the public key with a method called prime factorization. However, this is an extremely difficult problem: today's most powerful supercomputer would take about a year to solve such a challenge. For all practical purposes, such encryption is unbreakable.

Still, the Canadian Global Risk Institute estimated that there is a 'one in seven chance that some of the fundamental public-key cryptography tools upon which we rely today will be broken by 2026 and a 50% chance by 2031'. This can be caused by faster factoring algorithms, an increase in computing power or a large-scale quantum computer. A quantum computer should be able to do this, because it can find the prime factors of large numbers much faster than classical computers with the help of an algorithm developed by Peter Shor in 1994. Fortunately, large-scale quantum computers do not exist yet. But they are being developed, so a response is required. Two types of response are possible. One is to develop new encryption techniques that rely on information exchange over the classical internet; this is called classical post-quantum cryptography. The other involves using a quantum internet for creating encryption keys; this is called quantum key distribution.



Response 1

Response 2

Quantum key distribution

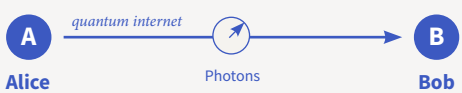
In 1984, computer scientists Charles Bennett and Gilles Brassard invented a scheme to securely distribute a key with the use of quantum mechanics. Since then a lot of versions of this scheme have been developed, which are all known as quantum key distribution. In quantum key distribution, parties create an encryption key over a quantum network. For sending the encrypted communication the parties still use the classical internet. Since quantum key distribution does not depend on the factorization of large numbers in prime numbers, the encryption keys that quantum key distribution gives cannot be broken by the Shor algorithm running on a quantum computer or by other fast algorithms for prime factorization.

How does quantum key distribution work?

In quantum key distribution usually single particles of light are used, called photons. There are two types of quantum key distribution with such photons.

type 1 - Preparation and read out

In type 1, a person A – let's call her Alice – prepares photons in a certain state and sends them over the quantum internet to person B, called Bob. Bob measures the photons to determine their prepared state. In this way Alice and Bob exchange a key.



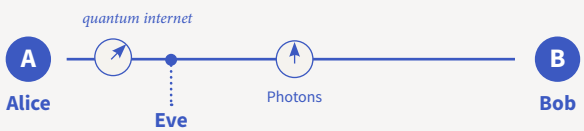
CRYPTOGRAPHY

type 2 - Device independent, entanglement-based

Type 2 is based on entanglement. Alice and Bob each have a qubit. They then establish entanglement between their qubits, using photons that they send over a quantum network. A key can be distributed between Alice and Bob using this entanglement between their qubits. Alice and Bob do this by both performing measurements on their qubits, and sharing (through a link over the classical internet) information about these measurements.

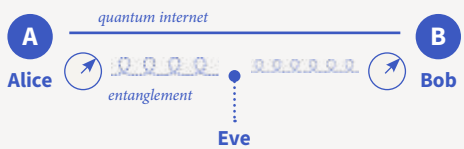
Safety type 1

This key exchange is safe. If an eavesdropper, let's call her Eve, wants to get her hands on the key, she needs to measure the photons that Alice sends to Bob. However, by measuring a photon, the state of the photon changes, and this change is something that Alice and Bob can detect. So Alice and Bob can check if Eve has listened in during the exchange of a key, and thus determine if the key is compromised. Compromised keys are thrown away; Alice and Bob only keep keys created in exchanges where no eavesdroppers were detected.



Safety type 2

This scheme is also safe. If Eve tries to eavesdrop, she will reduce the amount of entanglement between the qubits of Alice and Bob. And Alice and Bob can again detect this, and thus determine if the exchanged key is compromised. Moreover, it turns out that entanglement allows the scheme to be safe even if the devices that Alice and Bob use to distribute the keys have been maliciously prepared by Eve. Such schemes are called device independent.



The six stages of

Quantum networks

Quantum networks will go through different stages of development until they reach their full functionality. Recently, researchers from QuTech proposed a roadmap towards a full quantum internet, detailing six stages of development that are determined by the functionality available to the end nodes in the network.

Stage 0
Pre-quantum networks
The initial stage is that of *trusted repeater networks*. In these networks, end nodes that are directly connected can perform quantum key distribution, and end nodes that are connected by a chain of intermediate repeaters can also establish a secure key, provided that the intermediate repeaters are trusted. This stage can be regarded as a pre-quantum network, or zeroth stage, since no quantum information is exchanged between end nodes.

Stages 1 and 2
Proto-quantum networks
The first truly quantum stage, *prepare and measure networks,* makes the end-to-end delivery of qubits possible. This allows for instance to perform quantum key distribution between any two end nodes or secure login (see pages 17 and 34-35).

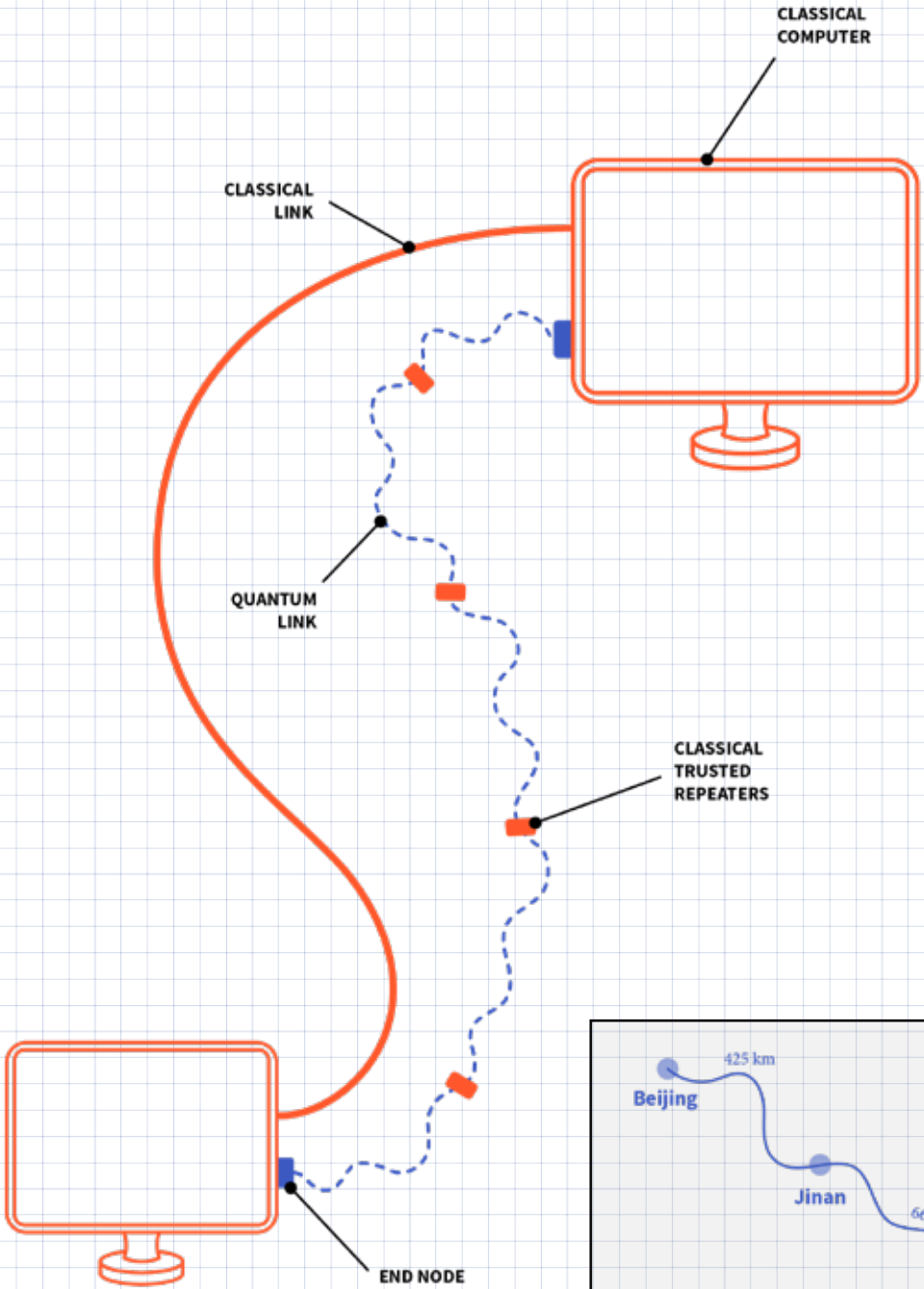
The second stage, *entanglement distribution networks*, allows for the distribution of entanglement between arbitrary nodes in the network. In this stage it becomes possible to implement the device independent version of quantum key distribution, based on entanglement (see page 17).

The first and second stages can be seen as stages of a proto-quantum networks since they make the first applications for quantum internet available. The next three stages enable further applications and are therefore advanced quantum networks.

Stages 3, 4 and 5
Advanced quantum networks
The third stage, *memory networks,* requires nodes to be able to keep quantum information in a quantum memory for a certain amount of time. At this stage, teleportation (page 25) and blind quantum computation (page 27) become possible, provided that a remote quantum computer is connected to the quantum network. In this stage, the implementation of quantum clock synchronization protocols, extending the baseline of telescopes, and quantum anonymous transmission (pages 36-37) also become possible.

To reach the fourth stage, *fault-tolerant few-qubit networks,* local operations and memory lifetimes need to be so good that a networked or distributed quantum computer (pages 36-37) can be implemented by connecting nodes from the network.

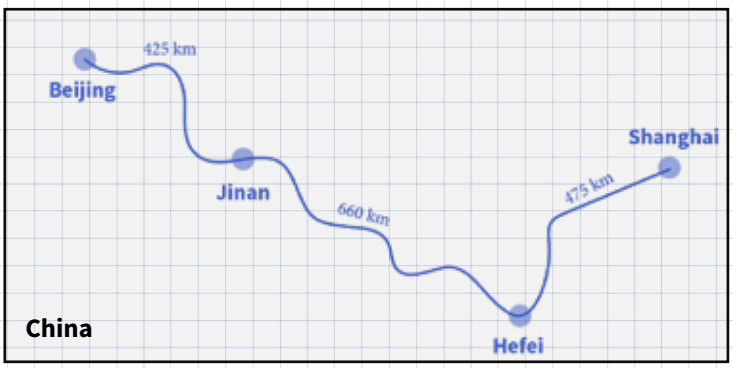
In the fifth and final stage, *quantum computing networks*, a full-fledged quantum computer is situated at each of the end nodes. In this stage, all quantum applications that we currently envision can be executed. For instance, this stage is necessary to implement quantum voting protocols (pages 36-37).

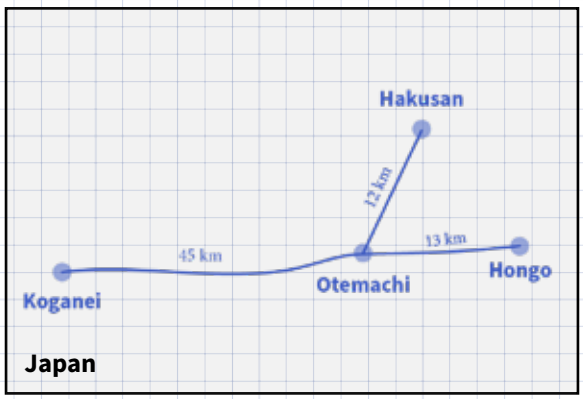


Pre-quantum network

Several pre-quantum networks are already in operation. Their quantum link is established through classical nodes, referred to as classical trusted repeaters, that are installed along the line. This setup is necessary, because quantum signals get lost when travelling through optical fibers. Typically, the classical nodes 'refresh' the signal at least every 100 kilometers.

Notably, Japan and China have implemented pre-quantum networks and quantum key distribution has already been performed there. This quantum key distribution, however, is not optimally secure because the classical nodes also learn the key while refreshing the signal, and need to be trusted.





Quantum network in Japan

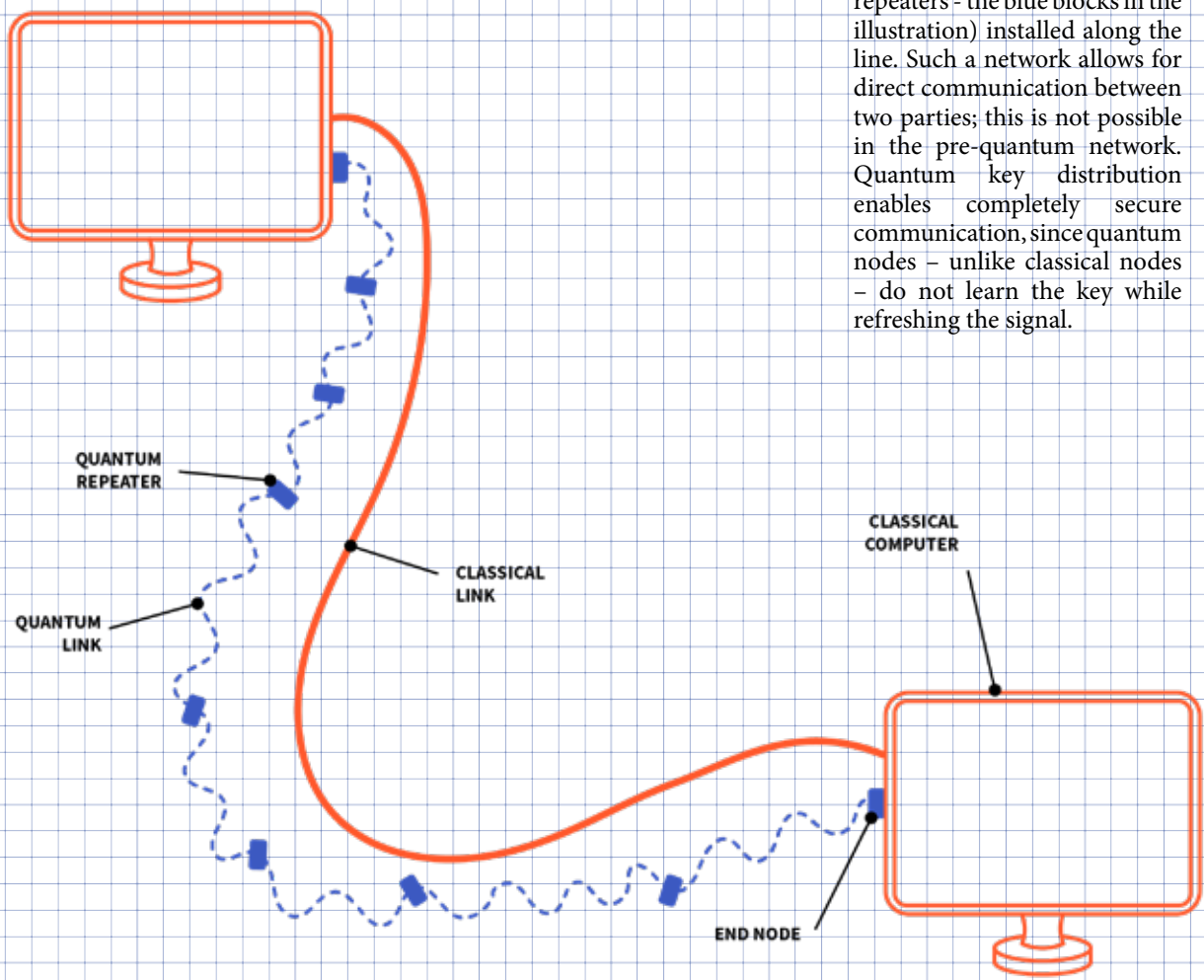
In Japan, an operation centre in Otemachi is connected with three other places that are situated 12, 13 and 45 km away. In 2010, a secure TV conference was demonstrated between Kogenei and Otemachi by performing trusted quantum key distribution.

Quantum network in China

In China, one trusted repeater network already covers a long distance: 2000 kilometre of optical fibre connects Beijing with Shanghai. This network is being tested for banking and commercial communications, such as linking up data centres or online shopping businesses.

Proto-quantum network

Instead of classical nodes, a proto-quantum network has quantum nodes (quantum repeaters - the blue blocks in the illustration) installed along the line. Such a network allows for direct communication between two parties; this is not possible in the pre-quantum network. Quantum key distribution enables completely secure communication, since quantum nodes – unlike classical nodes – do not learn the key while refreshing the signal.

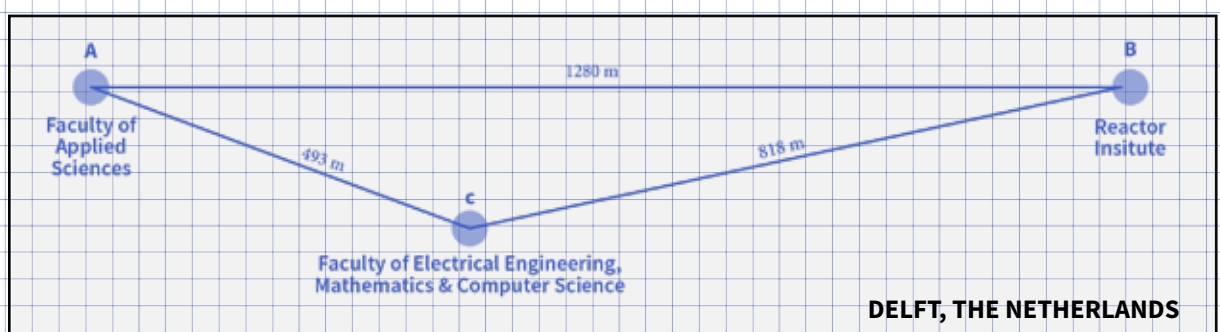


For more information on the entanglement distribution network in Delft:

Interested to learn more about entanglement?

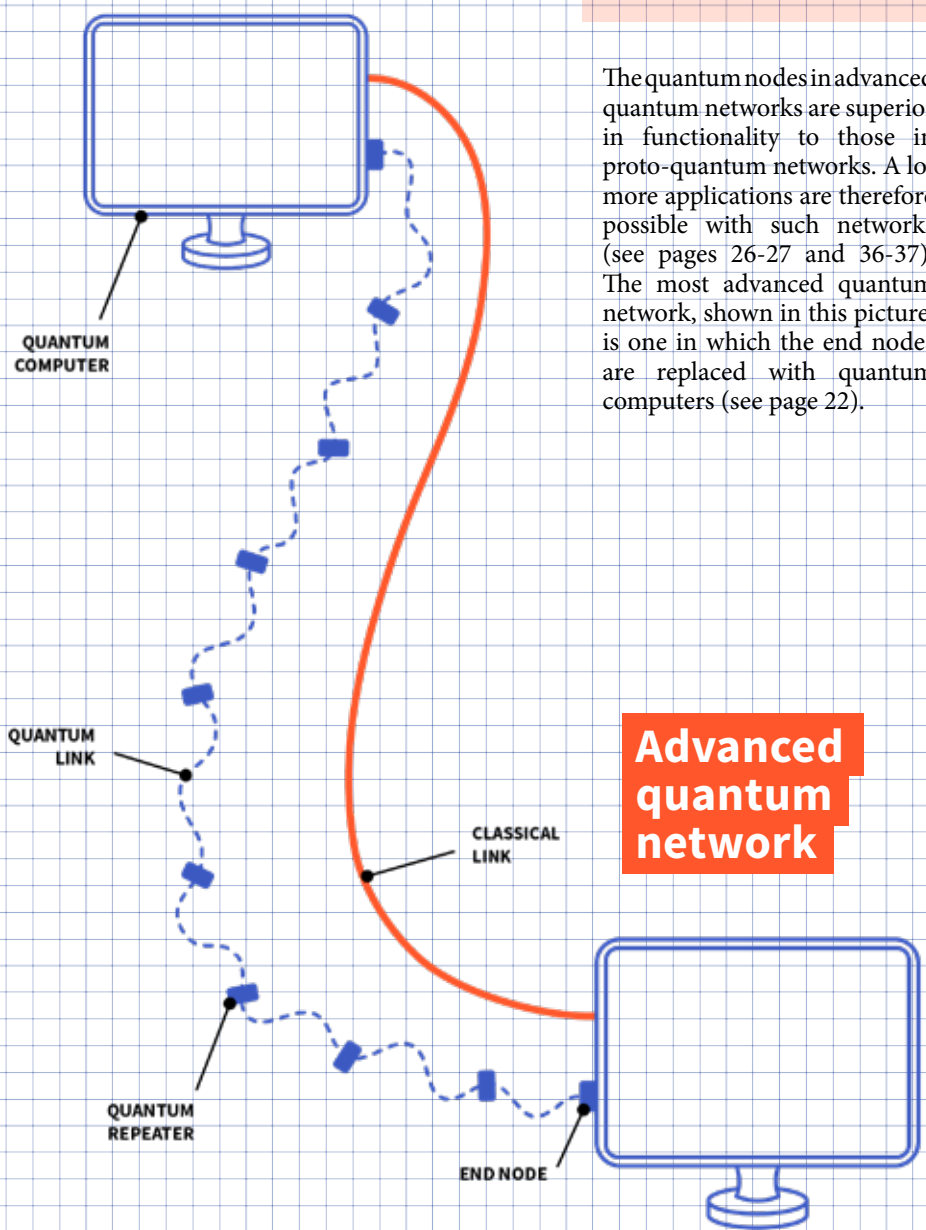
A quantum network with direct communication between the end nodes (end-to-end entanglement) is called an entanglement distribution network. In 2015, an entanglement distribution network covering a short distance was demonstrated in Delft. The two end nodes at positions A and B were placed 1.28 km apart. Entanglement between the end-nodes A and B was provided through position C.

An entanglement distribution quantum network enables the implementation of several tasks. Notably quantum key distribution, but also more mundane ones such as coordinated strategies to win online games (see the pages 36-37).



QuTech is working on realising an advanced quantum network in the Netherlands with quantum nodes placed at Delft, The Hague, Leiden and Amsterdam. These quantum nodes will function as end nodes as well as quantum repeaters; they therefore need three properties. First, a quantum node should have a quantum memory that can robustly store qubit states. Second, it should be possible to process quantum information with high fidelity within a quantum node. Third, the quantum nodes should be able to communicate via fibres that are currently used for our classical internet.

The quantum nodes in advanced quantum networks are superior in functionality to those in proto-quantum networks. A lot more applications are therefore possible with such networks (see pages 26-27 and 36-37). The most advanced quantum network, shown in this picture, is one in which the end nodes are replaced with quantum computers (see page 22).



Advanced quantum network

What is a quantum memory?

A quantum internet needs a memory to store the states of qubits. Such a quantum memory can be compared to the short-term memory that a classical computer uses to speed up the access to a program, the cache memory.

Without a quantum memory, a large quantum network would not be possible. Many protocols require memories and all network links would have to be established nearly simultaneously, which is very unlikely in larger networks. Any failure would mean that all quantum superpositions are lost and need to be re-created from the start. A quantum memory allows for the network to be established step by step, while storing the precious quantum states. This enables, for example, reliably sending quantum states by quantum teleportation.

How long a quantum memory should be able to store a qubit state depends on the time it takes for the communication to succeed in the rest of the network. A couple of seconds to a minute will probably be enough. While that is trivially achieved with classical bits, most types of qubits lose their state in a few microseconds. The quantum memory in the Delft quantum network can already keep superposition states for over 10 seconds. More research is underway to make sure that these quantum memories remain reliable even when the network links are operated at the same time.

Picture by QuTech

Quantum computing

What is a quantum computer?

A quantum computer can be compared to a classical computer, but instead of using classical bits it works with qubits. Quantum computers are expected to be very powerful. For instance, it is expected that quantum computers with a few thousands of good quality qubits can recover the private keys in public-key cryptosystems: a problem deemed intractable with classical computers. The computing power of quantum computers doubles with every good-quality qubit that is added. However, it is currently still a challenge to incorporate large numbers of interacting qubits in a quantum computer. Many companies are trying to build large-scale quantum computers based on different types of qubits. It is far from clear yet which one will turn out to be the ultimate qubit. In fact, large-scale quantum computers might even become hybrid systems, based on various types of qubits.

You might expect that we first need to build large-scale quantum computers that work with millions of qubits, before we can actually have a quantum internet. After all, classical computers also arrived before we could connect them via the classical internet. It turns out that history may not be repeating itself in this case: we expect to have a functioning quantum internet before having large-scale quantum computers. This is because a quantum internet can already connect quantum devices that contain a single qubit – and we are already envisioning applications for this.

Qubits: quantum computer vs quantum internet

A quantum computer needs very high-quality qubits, while a quantum internet already functions with lower quality qubits (with the help of the classical internet).

A quantum computer needs thousands to millions of qubits before it will be able to outperform classical computers for certain computations. A quantum internet can already outperform a classical internet on security with very few qubits

Quantum computers will nevertheless have an impact on the quantum internet. Once full-fledged quantum computers become available, the most advanced type of quantum network can be built: the quantum computing network. In this quantum computing network, quantum computers are linked to each other via the quantum internet. With large computing power, extremely difficult problems can be solved that can no longer efficiently be solved with a classical computer.

Examples are:

- Breaking widely-used public key cryptography
- Solving certain types of optimization problems faster, like optimization problems in data analytics
- Simulating molecules and materials more efficiently, which can aid a better understanding of diseases and the design of more effective medicines

The DiVincenzo criteria

In order to claim that you have built a quantum computer, the quantum computer should satisfy five criteria:

- *It should have well-defined qubits and be scalable*
- *It should be possible to initialize the qubits, to start computations with well-defined qubit states*
- *It should be possible to perform a universal set of quantum gates, to allow arbitrary computations*
- *It should be possible to perform qubit-specific measurements to access the end result of the computation*
- *Qubits must have long coherence times (the timescale for which superpositions persist)*

Examples of qubit technologies and industry involvement

Superconducting qubits

QuTech, intel, Google, rigetti, IBM

Silicon spin qubit

QuTech, intel

Topological qubit

QuTech, Microsoft

Single photons

Individual ions / atoms in a trap

IONQ, AQT

Qubits in diamond

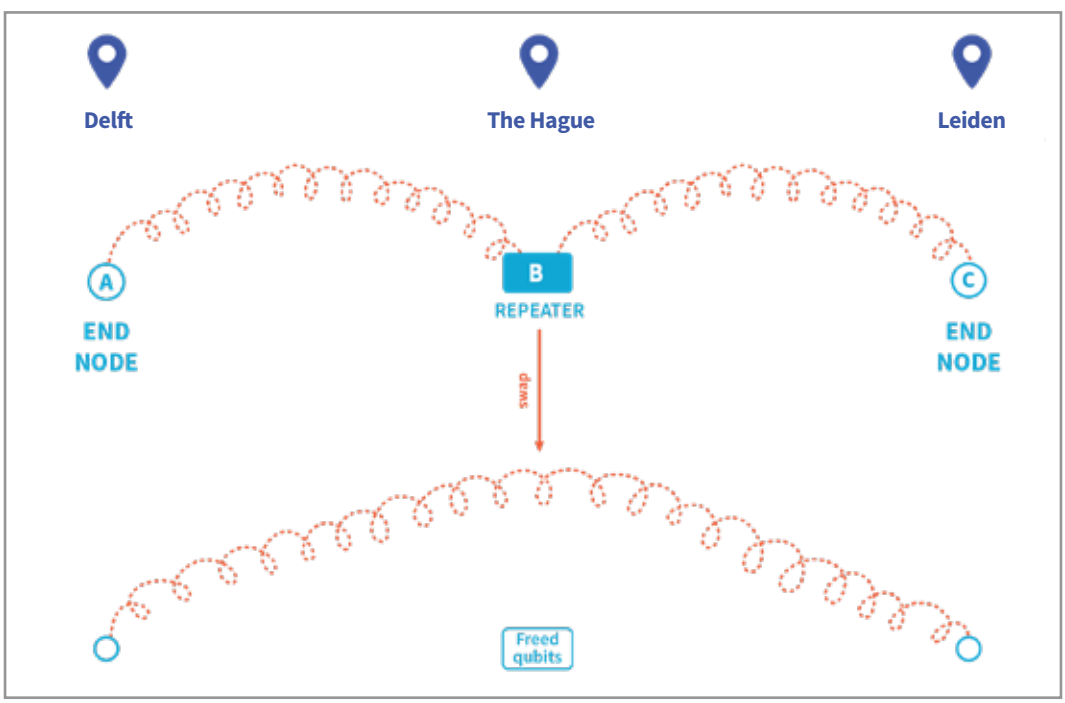
QuTech

The exponential power of qubits

Classical bits		Qubits
2xn		**2^n**
(2x2) 4	**n = 2**	*(2^2) 4*
(2x3) 6	**n = 3**	*(2^3) 8*
(2x4) 8	**n = 4**	*(2^4) 16*
(2x5) 10	**n = 5**	*(2^5) 32*
... ...		*... ...*
(2x100) 200	**n = 100**	*(2^{100}) 1267650600228229401496 703205376*

Quantum repeaters

In space, photons can travel for hundreds and hundreds of kilometers with a small probability of getting lost. This is a luxury that doesn't apply to fiber. Imagine that you have a photon source that releases 10 billion photons every second. With a fiber connection in which a bit less than one out of twenty photons gets lost every kilometer, after 500 kilometers the rate has dropped to roughly one photon arriving every second. After 1000 kilometers of fiber there is such an immense drop in the rate that you might not even be able to measure any photon in your own lifetime anymore: after 1000 kilometers of fiber around one photon will arrive every 300 years. Therefore, the signal needs to be refreshed.

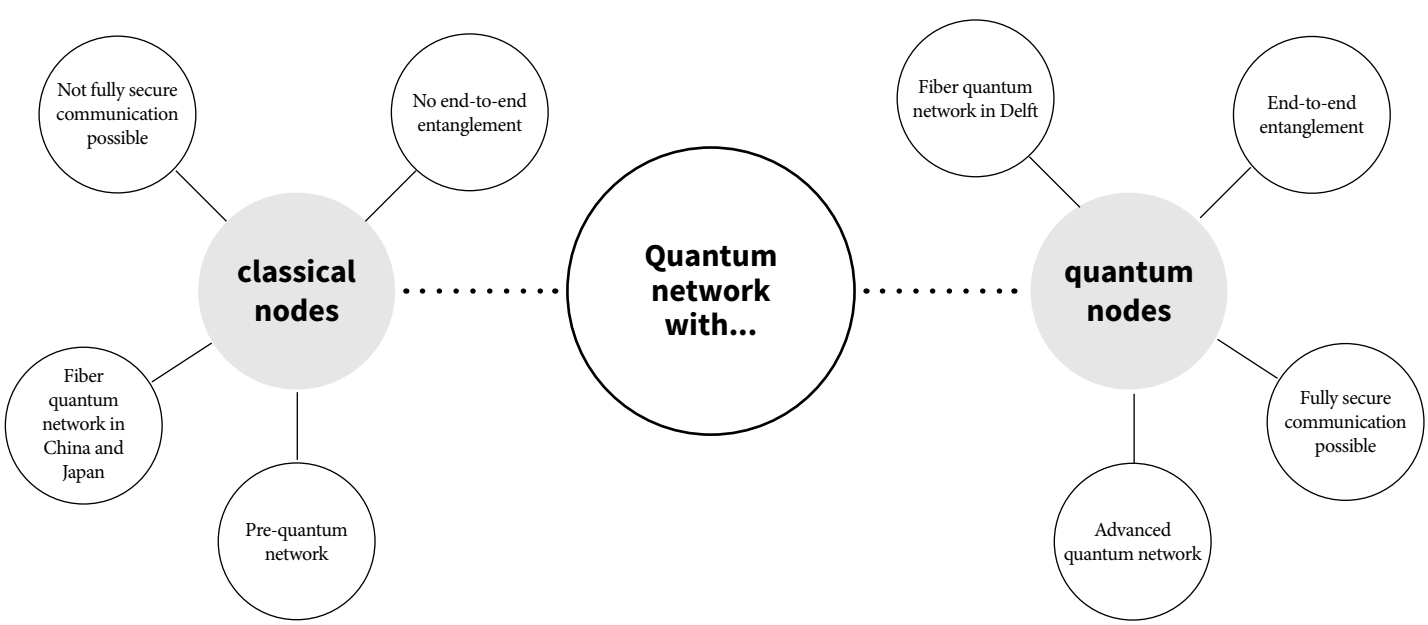


Refreshing the signal with classical nodes

In a pre-quantum network, such as the ones in China and Japan, this is the job of classical nodes. At the node, the photons that arrive are collected and their state is measured. Afterwards, fresh photons in the right state are sent towards the next node in the chain.

The next stage: quantum repeaters

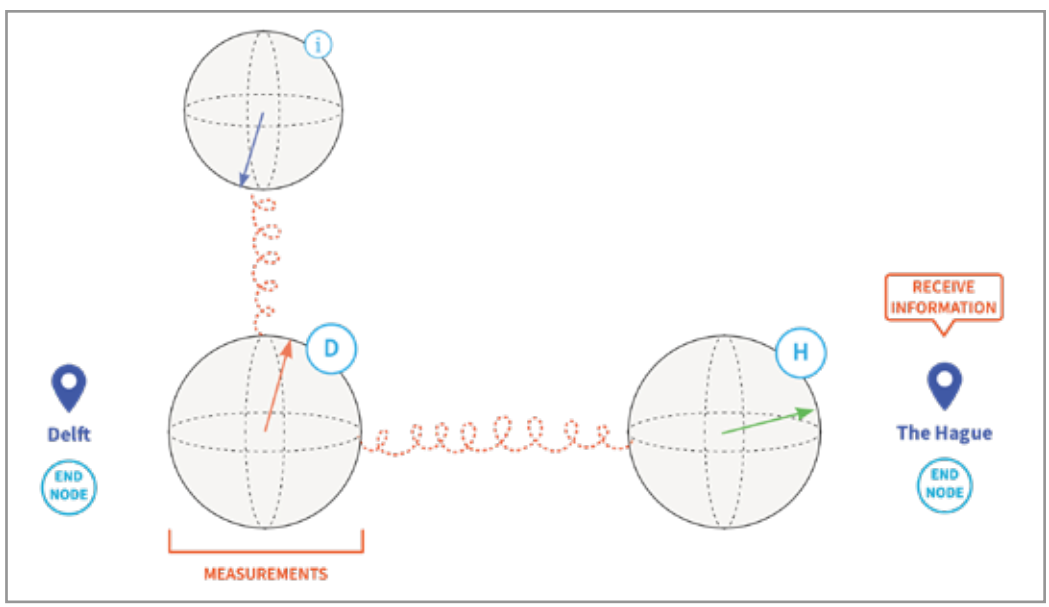
In stages beyond the pre-quantum network, the aim is to refresh the signal with a different kind of node: a quantum repeater. True quantum repeaters have not been realized yet, but in the near future the basis for such repeaters will be laid on the Dutch quantum network. In order to understand how quantum repeaters work, it's important to understand a different concept first: quantum teleportation.



Quantum teleportation

"Beam me up, Scotty"
— Captain Kirk, Star Trek

If you've watched Star Trek, or any other science fiction film where teleportation is commonplace, you probably already have an idea of what teleportation should look like: an object disappears and reappears somewhere else. But while teleportation in science fiction films often ignores physical laws, quantum teleportation works just because of that. Performing quantum teleportation means that a quantum state disappears on one side and then reappears again at the other side. The quantum state doesn't physically travel from one side to the other, but it is teleported. Also note that the state gets destroyed at the original location.
Quantum repeaters use this concept of quantum teleportation. Imagine that Delft and Leiden are part of a quantum network and they are connected via a quantum repeater in the Hague. First, entanglement can be generated between the end node in Delft and the quantum repeater in The Hague. Also, entanglement can be generated between the quantum repeater in The Hague and the end node in Leiden. Once both links succeed in generating entanglement, the quantum repeater can employ the following trick: it can use the qubit that is entangled with Leiden to teleport one qubit from The Hague to Leiden. In particular, it can teleport the qubit that is entangled with Delft. Hence, after performing the teleportation protocol Leiden obtains a qubit which is entangled with Delft.
This procedure is known as entanglement swapping.



Teleportation of information qubits

Suppose that we have a quantum network between Delft and The Hague. The qubits in Delft and The Hague, qubit D and qubit H, are entangled. In Delft there is another qubit, the information qubit, that we want to teleport over the network to The Hague. First, the entanglement between qubits D and H needs to be stored in a quantum memory. Afterwards, qubit D and the information qubit can get entangled. In Delft, we perform certain measurements on the qubit D and the information qubit and afterwards we communicate our measurement outcomes to the Hague.
Note: this communication with The Hague is classical, not quantum. After receiving the classical communication, the node at The Hague performs certain operations to compensate for the measurement outcome which lead to qubit H having the same state as the information qubit originally was. In other words: the information qubit has been teleported.

Big alternative

China is working on a quantum communication network in space. In space, there is negligible photon loss and photons can remain in a superposition state for a long time, meaning that no repeaters are needed. Recently, a trusted repeater network was established between a satellite and three ground locations, two in China and one in Austria, quantum key distribution has already been performed. In 2017, a secure videoconference was held between scientists in Austria and China with this network. Since the rate at which keys were generated did not allow for direct encryption, the keys were used to feed a symmetric cypher (Advanced Encryption Standard protocol), resulting in the secure videoconference lasting for 75 minutes.
Furthermore, the Chinese team has also demonstrated quantum teleportation from the ground to the satellite. Since fiber networks have the advantage of efficiently and conveniently connecting several users inside a city, the satellite has already been connected to the Chinese pre-quantum network.
A quantum network in space has two main drawbacks. The first is a low transmission rate since out of every 6 million photons sent from the satellite every second, only about one photon was detected on the ground. The second drawback is that today, a quantum network in space can only operate at night. Therefore, China's National Space Science Center is expected to launch other satellites that have stronger and cleaner beams such that it can also operate during the day.

Future scenarios

Classical network & Classical computer

Classical post-quantum cryptography

A gradual transition towards quantum-resistant systems and services

Quantum technologies are still in their infancy, yet we are already starting to see the first commercial products and services that make use of quantum technologies. Even though a large-scale quantum computer that can break existing cryptography schemes is likely to be more than 10 years away, it is imperative that industries and societies start preparing for the quantum era. This involves upgrading current cryptography schemes to post-quantum cryptography schemes, which requires software upgrades and very often hardware upgrades as well. This is a massive undertaking for organizations that deal with extensive infrastructure and legacy systems like, for example, banks and telecom operators. Most of these large organizations will need up to ten years to become fully quantum resistant. It will be a gradual process, not a big bang; initial focus will be on critical data and infrastructure. This means that there will be a time period of five to ten years, depending on the organization and speed of implementation, in which parts of their systems will be quantum proof and other parts will not be.

Tech consultancy companies will seize the opportunity and establish specialized quantum teams to help organizations become quantum-resistant.

Quantum network & Classical computer

Quantum Communication

Creating a fundamentally different internet

Although working in fundamentally different ways, the architecture of quantum networks will resemble classical networks: nodes with (quantum) processors, glass fiber lines and optical (quantum) switches to direct traffic to the right node. We can use high-quality fibers that are already in place today, and install additional hardware and software to create quantum networks. This will enable fully secure communication by creating entanglement on demand between any two users on the network. Initially, quantum networks will only be available between a few locations and have very low bit rates. They will primarily be used for quantum key exchange, synchronization and identification (more on these applications on pages 32-39). The first quantum networks will be owned and used by governments, big tech companies and telecom providers. Early adopters of commercial services will be organizations with sufficient budgets and a high need for secrecy. Examples are financial institutions, manufacturers and service providers in the defence industry, non-governmental organizations and maybe also criminal and terrorist organizations in disguise.

Over time, quantum networks will evolve into a full-scale quantum internet with higher bandwidths. Commercial quantum communication services will become more widely available and affordable, and we will have a quantum internet that co-exists with the classical internet.

We can't predict exactly when quantum technologies will become available, but we do expect breakthroughs that will make quantum applications feasible and viable in the coming decade. We highlight four scenarios in which quantum communication and quantum computers are – or are not yet – available. Keep in mind that, staying true to quantum theory, all four scenarios can exist at the same time.

Quantum Computing

Towards quantum advantage and beyond

Quantum computers will bring us computing power we have never seen before.
Universities, research institutions and tech companies like Google, IBM, Intel, Microsoft and Alibaba, are working hard to make quantum computers a reality. They are also working towards quantum advantage – also referred to as quantum supremacy – the point in time when a quantum computer can solve problems that a classical computer cannot (or takes so long that it is not economically viable). Besides breaking today's most widely used cryptography schemes, we don't know yet what the other killer applications for quantum computing will be. And since quantum computers work in fundamentally different ways, we need quantum programming – a new way of coding – and a new type of programming interface. Some organizations are making quantum computers publicly available over the internet to learn how people use it, and what they will use it for. Some of them combine classical and quantum computing in a single cloud platform, offering a virtual development environment for building quantum programs and running these on real quantum hardware.
Early adopters are expected to use quantum computers to solve challenges in chemistry. With the help of quantum computers, we can simulate chemical reactions and predict the properties of complex molecules that classical computers cannot handle. This will enable us to design new chemicals, drugs and materials instead of discovering them through endless experimentation.

Classical network & Quantum computer

Quantum Cloud

Unleashing the full power of quantum technologies

When combining quantum computing with quantum communication, blind computing becomes a reality. This quantum computation at-a-distance is called 'blind' because it is fully secure. Nobody in the network can intercept your data and even the people who own the quantum computer cannot see what type of algorithm you're running or what data you have. This offers benefits for governments, non-governmental organisations and corporations who want to solve computational challenges that are highly sensitive from a political or commercial perspective. However, it also poses a threat: criminals or terrorists can use blind computing to break (classical) encryption or develop new weaponry, for example. The combination of quantum communication and quantum computers may also bring quantum advantage closer to the present. Building a single computer with a high number of logical qubits is still very difficult, and most likely more than ten years into the future. But through quantum networks we can link multiple smaller quantum computers and by using this distributed computing, the system behaves like one virtual large-scale quantum computer.

Quantum network & Quantum computer

Bringing the quantum internet to life

An interview with Stephanie Wehner

Professor of Quantum Information at TU Delft

You are a thought leader on quantum networking. What first sparked your interest in quantum technologies?

I first learned about quantum technology a very long time ago, when I visited a public audience talk. I was immediately fascinated about the concept of quantum entanglement and the fact that qubits cannot be copied.

You are now a professor and the roadmap leader for Quantum Internet and Networked Computing at QuTech. What is your research focus?

My main research focus right now is two-fold. I'm working on defining a network stack, for which we've recently taken the first step by defining a link layer protocol. My other focus area is finding a scalable design, on how we can make a large-scale quantum internet a reality. For this, we built a simulation platform that can help us explore possible designs for a scalable quantum internet. This platform enables us to simulate, test and learn – for example – what hardware parameters are more important than others. To make a quantum internet a reality, we must combine science and engineering. This is why I have many different disciplines working together in my team. This fits QuTech's mission-driven culture, which means that we're organised around roadmaps instead of departments. Our interdisciplinary way of working is also very much appreciated by our students. As an example, QuTech's academy program for master and PhD students is open to all disciplines at the same time. Students from for example physics, engineering, and computer science work together on projects. They don't necessarily always understand each other right away, but they appreciate that they know different things and complement each other.

What do you see as the key challenges in developing a quantum internet?

One key challenge is to generate entanglement faster, that is, we want to achieve faster data transfer over such a quantum internet to make it useful. At the same time, we need to reinvent networking from scratch. In most research areas, researchers have a more narrowly confined research scope. They are working on software for existing hardware, or developing new hardware that will work with known software protocols. In our case, we're inventing the first version of quantum networks, all the way from application to hardware. This is massively complicated. And this is also why many parties are involved; it has never been done before, and all of the elements need to fit together.

What can we learn from the design of the classical internet?

We can learn a lot from the classical internet, for example how to prioritise and schedule data transmission and operations. We used this knowledge in the development of our link layer protocol. We can also learn from design mistakes that have been made. Of course, it is easy to say that in designing the quantum internet, we're going to do everything right from the start. But in reality, we want to make the first small quantum network happen in three years. This means we're making assumptions and pragmatic choices and it's almost impossible to foresee the impact of the choices we're making today. So even though we try to learn as much as possible from the classical internet, it is likely that we also won't get it right the first time.

To what extent will the roles in the quantum internet be similar to the roles in the classical internet?

I think that the role division between people who develop and apply a quantum internet will be quite similar. This also makes it quite complex to develop a quantum internet, because we need many different players to make a quantum internet available and useable. I expect that many of the traditional players such as infrastructure and service providers or network equipment manufacturers in the classical internet will also move into the quantum internet, but there will also be new players. Today, it is not yet clear which of the existing players want to move into quantum networks, and what role they want to play. In addition, their success will partly depend on how fast they will act. New players and start-ups, although they often have less resources available, are more agile and can move faster.

You initiated the Quantum Internet Alliance, and are also the coordinator. What is the Quantum Internet Alliance working on?

The Quantum Internet Alliance is working towards the long-term goal of realising a quantum internet. We strive to develop the technology to send qubits over long distances, for which we need to develop quantum repeaters. Another goal is to advance functionality, meaning that we want to go beyond quantum key distribution and run more complicated applications on the network. We are developing a software and network stack that can do fast control, and that allows people to write arbitrary applications in software. This is not the case right now; at the moment everything is ad hoc. We also work on a Blueprint for a pan-European quantum internet that will tell us what to do next.

We will test our software stack on a four node network, by doing a remote quantum computation in the cloud. Although we will use a small quantum internet and quantum computers with only a few qubits, this will be a proof of concept for blind quantum computing. It will be truly secure quantum cloud computation, where nobody can look at the data nor the algorithm that is being used. In the future, this can have use

cases like a manufacturer that wants to simulate a proprietary material design, but doesn't want the service provider who owns the quantum computer to find out what this material design is.

How will you deal with intellectual property that will be developed by the partners of the Quantum Internet Alliance?

We have 23 partners from academia and industry, but not everyone is involved in everything. The intellectual property resides with the partner(s) who developed it. Partners who are not involved can gain access during the project if their own development depends on such access. It is not yet clear what will happen after this phase of the Quantum Internet Alliance ends, that is, whether there will be a continuation with the same partners continuing to use the same intellectual property during the project.

Will the quantum internet bring about revolutionary innovations?

I believe so, since many applications are already known and we do not even have a network yet. Entanglement, for example, can help in the coordination of tasks. I don't know exactly how far you can push this, but I can imagine that there can be all kinds of new applications that will take advantage of this, even though they are difficult to envision today.
I believe that it is very important that already in this early stage of the development of a quantum internet, the technology is available to other people so they can experience how it works. If you look at the classical internet, then its success was largely derived by creative innovators who had access to the technology and who wrote programs to make this technology do fantastic new things like chatting remotely, sending pictures, or using Twitter. Today, the protocols and applications that people invented for a quantum internet are developed from pure theory. But this is not how successful applications usually come into existence. People need to be able to interact with a quantum internet hands-on, and play around with it to develop and try out new applications. I'm sure that the technology will spark off innovations, but we don't know yet what they will be.

How does Europe compare to other regions when it comes to quantum networking?

In advanced quantum networking, Europe has a leading position. We have more quantum communication expertise than in, for example, the US. In Europe we have many different viewpoints and many different people, which is beneficial for technology development. However, to move fast and maintain our leadership position, better alignment between parties involved in research and development would be beneficial. I think we can learn from the space business, where there is much more alignment on the deliverables and goals. As an example, many parties are working on a single satellite. In quantum technology, everyone is developing their own. If our efforts are dispersed, it will be difficult to achieve ambitious 'moonshot' projects.

There are many fears about disruptive technologies. Should regulators get involved already?

We shouldn't regulate things too early. If you regulate too early, you can confine the configuration space of technical development. Right now, we're really just trying to make it work, and we can't envision the entire impact, and the societal challenges it will bring. Nevertheless, it's really important that different stakeholders start thinking about possible implications right now, and learn from innovation test beds as soon as possible.

The Quantum Internet Alliance

The long-term ambition of the European Quantum Internet Alliance is to build a quantum internet that enables quantum communication applications between any two points on Earth. The goal is to develop a Blueprint for a pan-European entanglement-based quantum internet, by developing, integrating and demonstrating all the functional hardware and software subsystems. The Quantum Internet Alliance is a Quantum Flagship project.

For more information, please visit:
www.quantum-internet.team

The Quantum Flagship

With a budget of €1 billion, a 10-year timescale, and over 5,000 researchers from academia and industry involved, the Quantum Flagship is one of the most ambitious long-term research and innovation initiatives of the European Commission. The goal is to consolidate and expand European scientific leadership and excellence in quantum research, to kick-start a competitive European industry in quantum technologies and to make Europe a dynamic and attractive region for innovative research, business and investments in this field.

For more information, please visit:
www.qt.eu

Applications

Picture by QuTech

Types of encryption

Cryptography is the field that studies how to secure information. The security goals of the end users can be different and relate to secrecy, data integrity, authentication and non-repudiation.

Today's cryptography

Most of today's cryptographic protocols are secure through hard mathematical problems like the integer factorization problem, the discrete logarithm problem or the elliptic-curve discrete logarithm problem. This is the case for the most popular public key cryptosystems. However, some of these problems are not hard for quantum computers. In particular, a quantum computer implementing Shor's algorithm can solve the examples above exponentially faster than a classical one. Hence, while some instances of these problems cannot be tackled by today's most powerful supercomputer, a powerful quantum computer could tackle them and, in consequence, break public key cryptosystems.

Quantum cryptography

Quantum cryptography studies how to secure information leveraging quantum resources. The most important example is quantum key distribution (see page 17). It provides secure keys to distant parties that can, in turn, be used to achieve fully secure communication. When exchanging keys through quantum key distribution, eavesdroppers are detected immediately, and the exchange can be aborted.

Classical post-quantum cryptography

also referred to as quantum-proof or quantum-resistant cryptography.

Classical post-quantum cryptography proposes classical cryptosystems that are expected to be secure against attacks from quantum computers. One example is symmetric encryption schemes, which is only moderately affected by quantum computers. A quantum computer running Grover's algorithm can search for the secret key faster than a classical computer, but the speedup is moderate. It is believed that by doubling the key lengths current symmetric cryptosystems will remain safe even against quantum computers. Other solutions are lattice-based cryptography, hash-based cryptography, code-based cryptography, multi-variate cryptography and supersingular isogeny-based cryptography.

The first applications of a quantum internet are expected to be ones that better secure our communication.

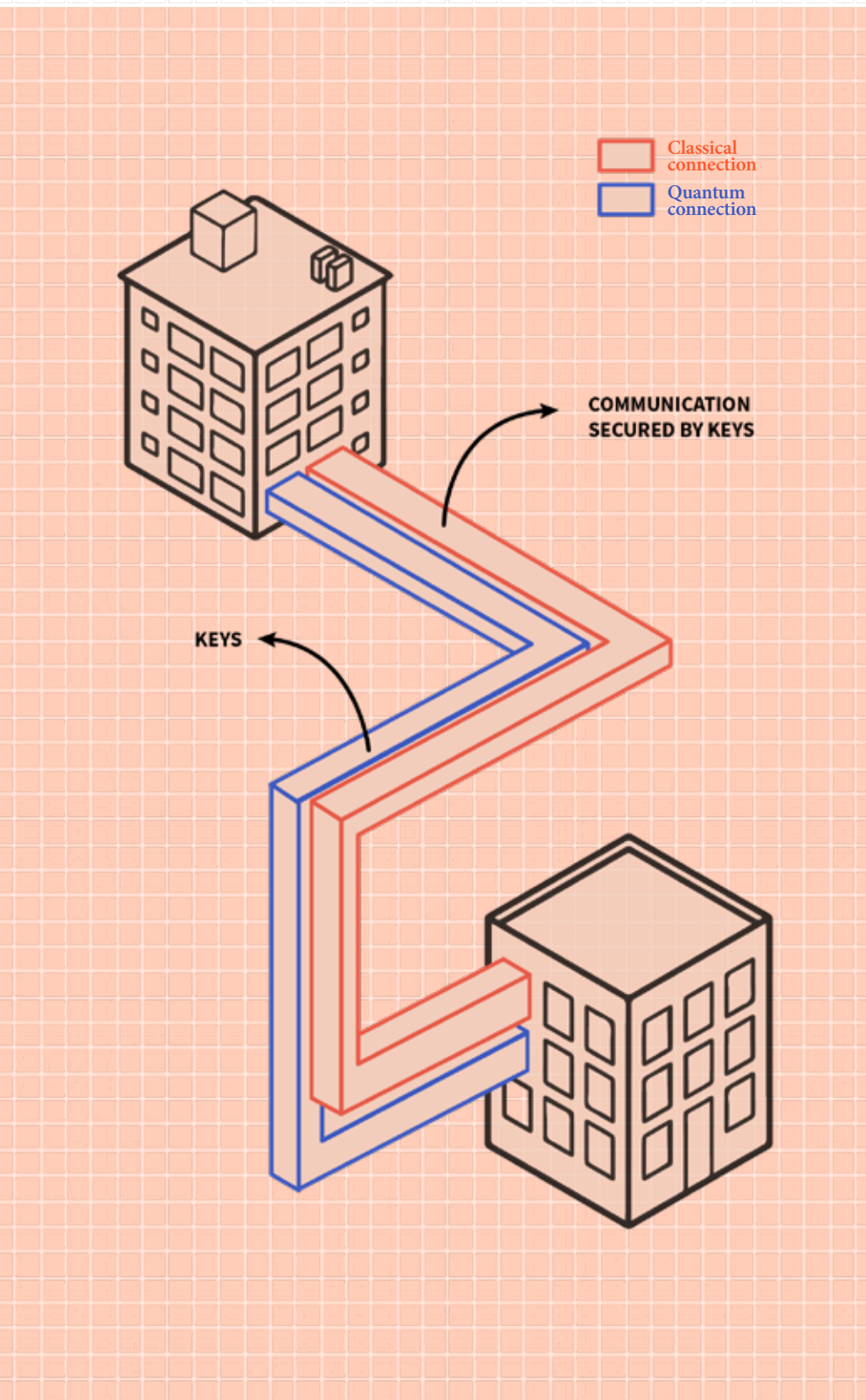
Secure communication in critical infrastructures

Our modern society relies heavily on the continuous, reliable and safe exchange of information sent over the classical internet. Every time you send a message via email or WhatsApp, every time you make a purchase on a website or upload your data to a tax organization, your information is sent via the classical internet; you trust that your information arrives and is not stolen by a third party. Much of the critical infrastructures in our society also depend on secure communication. Bridges, power plants, transportation systems, the banking system and governmental services such as the police and fire brigade, all need to exchange information for their smooth operation. Substantial interception of that information by hackers or adversaries would soon jeopardize the trust we have in society. Consider, for instance, a situation in which you cannot rely anymore on your email, electronic money transfers, the updates that companies send to our computers, or the equipment in hospitals or chemical plants.

Much of the information that is sent over the classical internet is currently made secure by keys that are created with encryption techniques that also exchange information over the classical internet. This allows hackers and adversaries to intercept that encryption information, and then to attempt breaking the encryption by finding the key. They can do so with decryption algorithms running on classical computers or, in the future, with algorithms that run on quantum computers. And once hackers have the key, the encrypted communication over the classical internet is no longer secure.

Quantum internet can block these decryption attempts by hackers and adversaries. It allows for the use of quantum encryption techniques that exchange information for creating keys safely over the quantum internet. With these keys communication that is sent on the classical internet can then be made secure again. The main quantum encryption technique is quantum key distribution (see page 17).

Secure communication



The first applications of quantum key distribution

It is to be expected that the first communication that is secured with quantum key distribution is communication between academic institutions, state institutions and between companies. The usual classical internet connections between these institutions and companies are then supplemented with quantum internet connections. And the quantum internet connections are used to generate encryption keys for securing communication over the classical internet. Later applications may enable securing the communication of individuals. For example, when banks connect their ATMs to the quantum internet, the communication between individuals and banks can be secured by quantum key distribution (see the next page).

Quantum key distribution already in use

Quantum key distribution is already in use. In Switzerland, quantum key distribution is used to secure the network between the places where the votes of elections are counted and stored. Quantum key distribution is also already in use in the Netherlands. In 2016, KPN established a safe network between datacenters in the Dutch cities of The Hague and Rotterdam by using quantum key distribution. In the future, quantum key distribution is expected to be used in more cases, like for auctions, elections or contract negotiations.

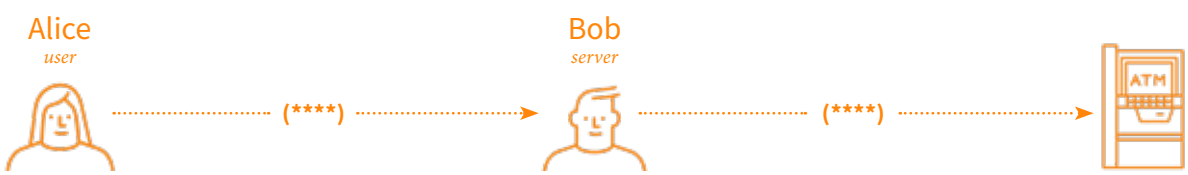
Secure login in networks

One application of the quantum internet is to obtain fundamentally secure communication via quantum key distribution (see page 17). With a few changes in the quantum key distribution scheme, another application of the quantum internet becomes available: secure login. This means that you can, in a fundamentally secure way:

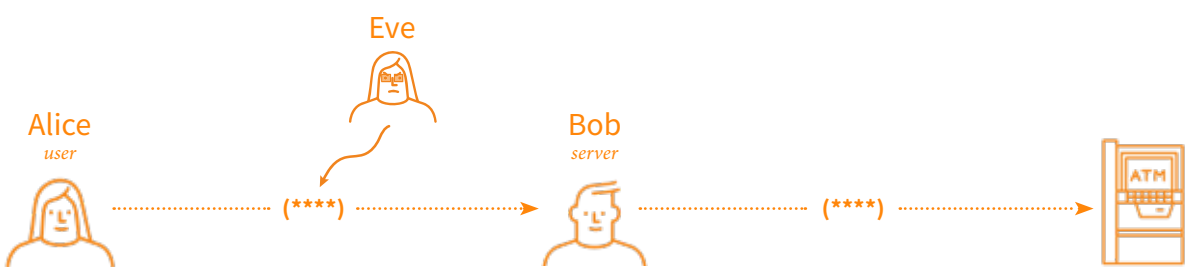
Identify the party you're communicating with over the network.

Prove your own identity to the other party.

Everyday examples of securely identifying users and servers at networks are numerous. In ATM usage, for instance, a bank needs to establish whether a user is the client they say they are, while the user wants to avoid disclosing any information to any party except for the bank. Or when you open your email account, the server needs to know you are the person you say you are, and you don't want your login information to be exposed to a fake website trying to steal your data. On the classical internet, identification is done by a user – let's call her Alice – typically sending her password (or other credentials) to the server – call it Bob. The disadvantages of this are that the server Bob gets the password over the internet connection between Alice and Bob. More sophisticated schemes use the password in combination with cryptographic schemes based on the hardness of certain mathematical problems such as factoring. Many of these schemes are not safe against adversaries with a quantum computer. This allows malpractices in which a third party – call her Eve – aims to intercept this communication with the password, either by eavesdropping on the line between Alice and Bob, or by phishing through presenting a fake server to Alice.



Alice sends her password to the server, Bob.



Eve aims to intercept this communication and steal the password.

A more ideal login protocol would be one in which Alice does not send her password to the server Bob, yet that allows Bob to verify that Alice is in possession of her password.

Quantum information technology makes such a protocol possible under reasonable conditions. More precisely, it allows for a protocol in which Alice and Bob are given a password and by which Alice can identify herself numerous times. Under such a protocol:

1

Alice always convinces Bob that she holds the password

2

An imposter pretending to be Alice can only convince Bob that they are Alice if they guess Alice's password correctly

3

If the imposter's guess of Alice's password is incorrect, then that is the only thing the imposter learns

4

A fake server presenting itself as Bob to Alice does not acquire information about the password of Alice either, beyond that the guessed one is indeed wrong

5

An eavesdropper doesn't learn more information than the Alice imposter and the fake Bob server

The protocol is secure if we assume that the technological abilities of the eavesdropper are somewhat limited. Broadly put, the eavesdropper can have a quantum computer, but that quantum computer should have a limited amount of memory, or should have a memory that is slightly noisy. These assumptions only need to hold during the execution of the protocol.

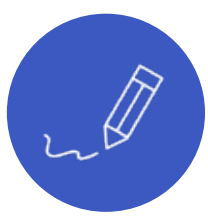
With such a protocol users and servers can regain confidence about the identities of the users and servers they communicate with. This would limit the abilities of users and servers that fake their identity and thus be a major improvement of security as compared to the classical internet.

Secure anonymous transmission

In communications, anonymity is a property where the identity of the sender and/or the receiver of a message needs to be kept secret. It is of importance in such communications as review processes, job applications, surveys and elections. One classical solution for anonymous transmission is to use a trusted third party that relays the message from sender to receiver while removing or not revealing any information about the sender. Other classical solutions rely on using many different intermediate parties who transfer the message, making it more difficult to find the sender's identity.
Quantum anonymous communication is a protocol that guarantees that a sender can send a message to a receiver, both being part of a bigger group, in such a way that the receiver or anybody else cannot tell who was the sender. It also guarantees that the information that was sent has not been tampered with, and that the receiver is only known to the sender.
In quantum anonymous transmission a multi-party entanglement is set-up first, e.g. by randomly selecting one party to set-up entanglement with all other parties in the network. Then the sender designates a receiver, by sending classical information to all partners. If all parties in the group follow a certain protocol using this information, an entangled link between sender and receiver becomes established. This link can then be used to send information anonymously to the receiver and the information is protected from an eavesdropper. Furthermore, dishonest participants (who do not follow the protocol) will cause the mechanism to abort, but no information about the sender, the receiver or the message can be learned from this.

Secure voting

Using quantum entanglement and quantum key distribution, different flavors of quantum secure anonymous voting can be realized, such as simple yes/no votes with multiple parties or more complex balloting systems, with ballot verification, casting multiple ballots, etc. Note that different protocols can have very different security characteristics or assumptions.



Quantum digital signature

Your passport, your debit card, your credit card, your driver's license, your employment contract and many other official documents in your life need your signature to become valid. An equivalent of the handwritten signature in the digital world is called a digital signature. A quantum version of the digital signature exists: a quantum digital signature. It allows you to identify yourself in a secure way by using quantum cryptography. Therefore, it becomes impossible to pretend to be someone you are not, making this a very secure version of your signature.

High-precision timing for Very Large Base Interferometry (VLBI)

High-precision timing plays an important role in applications such as Global Positioning Systems (GPS), gravitational wave detection systems and radio-astronomy systems based on Very Large Base Interferometry (VLBI). The VLBI system consists of several radio telescopes that observe the same part of the sky. The larger the distance between the telescopes (this distance is called the interferometry base), the better these telescopes can distinguish two closely spaced sky objects, like pulsars or quasars. Ultimately, you would like to place the radio telescopes on the opposite sides of the Earth, or, even better, to put them on the satellites positioned above the opposite sides of the Earth. However, for correct results, the local clocks of the telescopes in the VLBI system should be synchronized, and should maintain this synchronization for a long time.
The synchronization of classical atomic clocks is done by exchanging timing signals. The accuracy of the synchronization is limited by the uncertainty in the timing, which by itself is limited by the signal- to-noise ratio of the timing signals, but also by fluctuations in the transportation time of the signal between the clocks (timing jitter). Clock synchronization of GPS systems using satellite-based timing synchronization achieves a timing accuracy of about 500 picoseconds (2 billionth of a second). Fiber-based timing synchronization protocols achieve a timing accuracy of a few picoseconds.
Even better timing accuracy can be achieved by using entangled photons to synchronize distant clocks. Such quantum clock synchronization protocols have been investigated for bi-partite and multi-

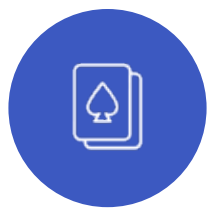
partite synchronization. Experimental tests with quantum clock synchronization have shown timing accuracies below 1 picosecond, which is about 500 times more precise than classical satellite-based timing synchronization. Theoretically, quantum clock synchronization can improve accuracy with another factor of 100, which would greatly enhance the performance of the applications relying on distant clock synchronization, such as gravitational wave detection as well as many other applications.

Gravitational wave detection

In 1916 Albert Einstein predicted that massive energetic events in the universe, like colliding neutron stars, cause ripples in space-time. In his theory, these waves travel through the universe like ripples on a pond, and pass our own planet. In principle, these waves can be measured at the Earth's surface, but the wiggling of space-time on Earth would be very small, smaller than the size of an atom. The measurement of gravitational waves gives us essential information about the creation of the universe, the life cycle of galaxies in the universe and a validation of Einstein's theories.
Because these signals are so small, it took almost a century before mankind was able to build systems sensitive enough to detect gravitational waves: in 2015 the LIGO observatory was the first to detect gravitational waves.
The LIGO observatory consists of two large interferometers placed thousands of kilometers apart. Each of these interferometers is designed to measure tiny changes in space-time caused by gravitational waves. A basic interferometer consists of a laser, a beam splitter that splits the light from the laser in two directions, two arms (each 3 kilometers long), mirrors at the end of each arm and a detector. The light reflected from both mirrors travels back to the beam splitter where it recombines (interferes) and hits a detector. Because the light travelling through the arms are waves, the detector shows a specific interference pattern. This pattern is extremely sensitive to changes in the length of the arms. The LIGO interferometers are designed to measure changes in the length of the arms much smaller than the size of an atom. This is sensitive enough to detect gravitational waves.
The sensitivity of these interferometers can be further increased by using squeezed light. Squeezed light is a quantum-mechanical effect by which the noise limit of the phase of the signal can be reduced to values lower than would be possible with classical light, by squeezing some parameters of the light (the phase quadrature) at the expense of increasing the noise in other (the amplitude quadrature).
The LIGO detectors are based at different locations around the world to validate that a detected event is really caused by a gravitational wave. Additionally, timing synchronization allows for various control systems along the optical arms of each interferometer, which is crucial for the operation of the LIGO system. This synchronization is done using the most accurate atomic clocks and the GPS system. Improving the synchronization using quantum communication systems will significantly improve the system.

Distributed quantum computing

Multiple small quantum computers can be linked together in a distributed quantum computing system via quantum connections. Note that a cluster of quantum computers connected by classical connections cannot be considered a distributed quantum computer, because entanglement between the computers is required to obtain an increase of computational power. Small quantum computers linked by quantum connections could be a stepping stone to future large-scale quantum computers.



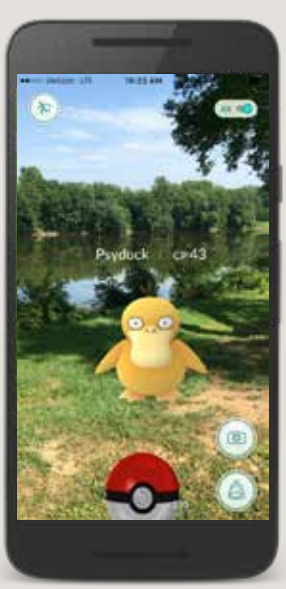
Cheating an online game of bridge

While it is debatable whether 'mind sports' are actual sports, the International Olympic committee recognizes two of them as such: chess and bridge. Bridge is played all around the world, but the popularity of the online version may vanish quickly once a quantum internet arrives. After all, who would want to play a game in which the opponents can easily cheat? The advent of a quantum internet calls for the rules of bridge, as defined by the World Bridge Federation, to be updated in order to prevent cheating in the online version. In bridge there are four players named North, East, West and South. North & South and East & West form a team. Cards are shuffled and distributed equally amongst the four players. The game starts with an auction and finishes with playing the hand. In the auction, each player bids on the number of tricks they think they will be able to get. The goal of the game is to guess the minimal number of tricks you can obtain as a team and take on the optimal contract to achieve that. This auction is tricky, because so many different deals are possible. However, it has been shown that with the help of preshared entanglement, team members can share information about the cards they hold more efficiently and are therefore able to cheat in the online version of bridge.

Quantum enhanced GPS

Global Positioning System

The Global Positioning System (GPS) is a global satellite system that enables us to define a GPS receiver's location anywhere on Earth.



All it needs is line of sight with 4 of the 31 GPS satellites that are circling the Earth. Developed and operated by the US Government, it became available for civilian use in the 1980s. Like with many new technologies, the scientists and engineers who developed the system could never have imagined what it would be used for 30 years later. Today, many businesses rely on GPS for their operations. It is used to navigate vehicles, to map forests and agricultural lands, to locate people in need of assistance, to track movements of wildlife, packages, containers and vehicles, and countless other applications. Location-based services have become part of everyday life. We use our smartphones to determine where we are and how to get to our target destination, to measure speed and distance when we go running, to check the whereabouts of our pets, or to capture creatures in Pokémon Go.

But GPS isn't perfect yet. It is vulnerable to cyber-attacks, and doesn't work flawlessly in urban areas. Moreover, its accuracy can be influenced by the US government, which is one of the reasons why the European Union is implementing the non-military Galileo global navigation system. The accuracy of this system will be approximately 1 meter, but quantum technology can improve this even further.

Picture by cako74

Interested to learn more about atomic clocks?

Atomic clocks

Did you know that GPS satellites have atomic clocks on board? And that atomic clocks are based on the laws of quantum mechanics? Learn more about GPS and atomic clocks in this 5-minute animation from TED- Ed.

More accurate GPS

GPS relies on atomic clocks. By measuring the time it takes to receive a time signature from a specific satellite, and doing this for four different GPS satellites, a GPS receiver can determine where it is on Earth. The US government commits to broadcasting the GPS signal in space with a global average user range error (URE) of less than 7.8 meters with 95% probability. Although the actual performance of the GPS system is better, most GPS-defined locations are still off by a few meters. This is partly caused by small variations that occur in atomic clocks on board of GPS satellites. A signal travelling at the speed of light takes about 70 milliseconds to reach you, so you can imagine that the slightest deviation between clocks can result in a location measurement that is off by meters. If clocks on board of satellites did not regularly synchronize, GPS performance would rapidly deteriorate and would be useless in a matter of weeks.
In the future it will be possible to use quantum communication technology to synchronize more accurately, transferring time information directly between the quantum memories in GPS satellites. The result? Pinpointing your location with much higher accuracy, theoretically up to 15 centimeters.

Safer GPS

GPS is so ubiquitous that failure of the system will have a huge impact. Unfortunately, there have been events of hacks and spoofs in the past. Besides the economic impact, these also create potentially dangerous situations, e.g. through malfunctioning air traffic control. With spoofing, the receiver gets false data, resulting into a false location and/or a false time. There have been recent events where GPS signals told ships they were on land, while they were actually at sea.

By using entanglement and quantum communication, we can be sure the time signature is authentic, improving safety for all.

A quantum alternative to GPS

GPS doesn't work if you're indoors or if you do not have satellites in sight: in between tall buildings, you will have a hard time getting a reliable GPS signal. Quantum technology may solve all this.

A special type of quantum sensors – quantum accelerometers and quantum gyroscopes – can be combined into quantum autonomous navigation systems. Such a system may enable location tracking without the aid of GPS satellites. Classical autonomous inertial navigation systems are already used on ships, aircraft, cruise missiles, and even in smartphones. They detect acceleration, movement and orientation, but they are too inaccurate to be a sole source of data for navigation. Quantum autonomous navigation systems, on the other hand, are extremely accurate. Using a starting point as a fixed reference, data from a quantum navigation system will give us all the information we need to accurately determine where we are.
Benefits of quantum navigation and positioning systems over GPS are improved accuracy, no reliance on satellite, indoor usage, less vulnerability to hacking and no sensitivity to electromagnetic pulse attacks (which would happen for example after an atomic attack, most likely causing GPS systems to stop working).

Today, the equipment needed for quantum inertial navigation systems is large, complex and costly, but this will improve over time. First, we expect commercial availability of quantum enhanced navigation equipment, combining GPS and quantum sensors, to navigate large vehicles like cargo ships and trains. As the technology further develops, devices will get smaller and will eventually become suited for smaller vehicles and other applications. Maybe one day we will even have a quantum autonomous positioning system in our smartphones.

Picture by Jose A. Bernat Bacete

Impact & governance

The possible dark side of quantum communication technologies

We assume that quantum technologies will progress rapidly, and in the near future will reach the level where they can significantly impact society. Most of this magazine discusses the bright side of quantum technologies, however there is also a possible dark side. Like any other technology, quantum technologies are neither positive nor negative; as any technology per se they are neutral. The extent to which quantum technologies will impact society, whether positively or negatively, will be defined by how humans apply them. Cyberpunk-style scenarios, like megacorporations using quantum technologies to seize all societal control and eliminate governments, are rather far-fetched: the majority of modern countries have the ability to prevent this. But let's take a look at potentially unpleasant changes that quantum technologies could realistically bring to society: our 'doom scenarios'.

Most of our doom scenarios are based on disruption of the currently existing balances:

- The balance between society, government, and business.
- The balance between the protection of sensitive information from open access (personal, medical, military, governmental information, etc) and making non-sensitive information openly accessible (e.g. to ensure control of society over government officials).

Our doom scenarios are possible courses of events where such balance is greatly disturbed, and cannot be repaired by the usual everyday means of governmental or societal control.

We do not base our discussion on predictions about which quantum technology will come first, when, or where. Such predictions are rarely successful. Many of the topics we discuss are based on unsolved scientific problems: for instance, it is not yet proven that quantum computation is exponentially faster than classical computation for solving specific mathematical problems. Also, it is possible that new developments in computer sciences will create efficient codes that cannot be broken by quantum computers, or require extremely large-scale quantum computers, which would keep sensitive information safe for much longer than expected. Of course, not all doom scenarios are equally possible: in fact, we consider most of them to be unlikely. We include them because understanding the possible negative impacts of quantum technologies can help society at large to prepare for this possible future, and as a result gain a better control of the situation, or even prevent things from happening when the time comes.

Bad guys gain access to vital infrastructure

The most obvious, and most often discussed, doom scenario is based on the possibility of a quantum computer breaking existing cryptographic codes, enabling unauthorized access to protected information. If this happens, it may become easy for criminals to get unauthorized access to secure facilities, to implant malware or to disguise malware as software upgrades, etc. The most disruptive situations may occur if criminals or terrorists get access to vital facilities: energy plants, water supplies and water management, air and railroad traffic controls, etc. This can bring entire countries and economies close to a standstill for prolonged periods of time. Equally disruptive – although in a different way – is the situation where criminals or terrorists gain access to protected military or law enforcement information, enabling them to outsmart their opponents.

Increasing power gap between rich and poor countries

Many governments will take measures to protect themselves from new security threats caused by quantum technologies. It is most likely that developing countries will lag behind in adopting advanced cryptographic approaches (classical or quantum). Even in developed countries the required changes in the computer networks and infrastructure will take a long time, given the large scale of the upgrades, and the associated financial expenses, manpower, and time needed. Developing countries will struggle to take their level of security to the next level. Especially countries that are rich in natural resources and have instable political systems will become more vulnerable to espionage and corruption.

Old secrets will become known

If quantum computers become a reality, and they are indeed able to easily break today's encryption methods, we can be reasonably sure that the military and law enforcement agencies will be vulnerable, for some time to come, to other governments, criminals and terrorists possessing advanced quantum technology-based tools. Initially, parties will use their knowledge of sensitive information to exert political power. There may be blackmail on a strategic political level at an unprecedented scale. Archived diplomatic, military, or police information that were encrypted with older cryptographic tools, may be very damaging if they are decrypted and become publicly available. This may lead to a massive crisis of trust between citizens and their government, which will result in political instability and new political parties seizing control. Some claim that the quantum computer is the digital equivalent of the atomic bomb. Whether the effect will be this destructive needs to be seen. Nevertheless, scientists and regulators need to be aware of the power that will be unleashed.

Impact financial systems

Money has become a digital asset and most banking transactions are done online. Economists estimate that less than 10% of all the money in the world exists as bank notes and coins. Cyber criminals targeting financial gains may use quantum technologies to hit financial networks and online banking: consider, for instance, primitive online theft at an excessive scale, that would render online banking transactions practically useless and thus seriously damage or completely cripple the modern banking system. In a similar way, unauthorized access can cause massive disruptions in the functioning of major banks and commodities/stock exchanges.

New weapons that should never see the light of day

Rogue states or advanced terrorist groups might get access to blind quantum computing. Quantum computers are especially good at designing new materials and molecules – for good and for bad. Blind quantum computing services, accessed through 100% secure communication, can enable users to design new kinds of modern warfare, e.g. chemical or nuclear weapons, without anyone knowing about it, or use available large-scale computational facilities for advanced code breaking efforts. In a similar way, it may give terrorist groups or organizations, or rogue states, access to major military-oriented computational facilities to gain information about such development performed by other groups/countries, or possibly sabotage such computer-aided design and development.

Governments losing their grip on criminal organisations

If secure quantum communication solutions become available to criminals or terrorists, they will render existing surveillance and wiretapping tools used by the military and law enforcement agencies useless. It is possible that commercial quantum communication services become available before legislation on these technologies is in place, limiting the surveillance power of official bodies.

Governments becoming less transparent

Quantum technology offers governments secure cryptography and communications that prevent transparency and control by the public. This could make corruption within governments much less risky and more tempting.

Governments gaining too much control over their citizens

Exclusive access of some government agencies to the quantum-enabled tools may greatly disturb the intra-government balances, giving some agencies too much political power and weight. Also, governments may overextend their authority by using massive large-scale data processing and almost real-time decrypting abilities enabled by quantum technologies, thereby penetrating too much into the lives of people and fostering totalitarian regimes.
On the other hand, if citizens have access to 100% secure communication, this greatly increases the individual freedoms and an individual's ability to avoid governmental control, which counteracts the tendency of many governments towards deep invasion into the private lives of people.

Increasing power of large tech companies

Quantum technologies are being developed by big tech companies, research institutions and universities. Although findings from research done by universities are in the public domain, big tech companies often invest heavily in such research. As a result, big tech companies have early access to findings and can influence the focus of research to fit their own interest. Quantum technologies may provide many new opportunities in the areas of development of new materials and weapons, large-scale analysis of critical sensitive information and surveillance, secure communications, quantum-enabled computer sabotage, etc. Corporations may offer these new opportunities to governments in exchange for more favourable treatment, or for other political advantages, thus gaining too much political leverage. At the same time, the quantum technologies may make these corporations less amenable to conventional means of governmental and societal control.
Note that this may happen even without explicit bad intentions on the side of these corporations, simply in the normal course of legitimately pursuing new business advantages, seeking for better deals with the government, and ensuring a better position in the market. It may be too tempting for weaker governments to use tit-for-tat policies when dealing with such corporations, and surrender too much power to large businesses in exchange for short-term political gains. In the situation of strong international competition, some governments may even actively encourage this approach, hoping to exploit the quantum technologies offered by the corporations in order to advance their national or international political status.

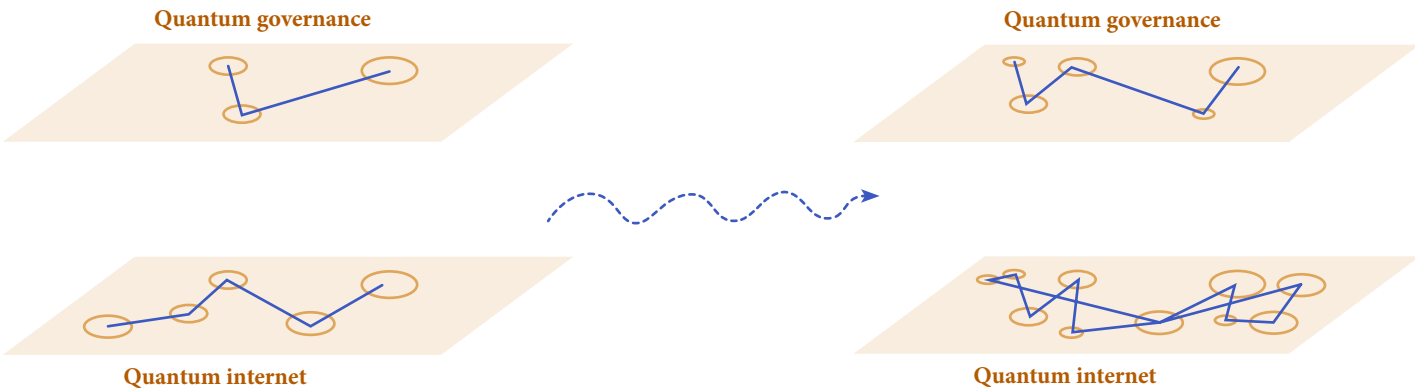
Governance

security
safety
resilience
trust
privacy
equal access
net neutrality

We want the internet in its current classical form to comply with our public values. These values include security, safety, resilience, trust, privacy, equal access and net neutrality. Over time, all kinds of governance mechanisms have emerged so the operation and development of the internet can better meet our values and avoid undesired effects. The classical internet consists of physical infrastructure such as cables, data centers, antennas, routers, terminals and sensors, and a protocol stack to ensure that nodes can find each other and route data. And its distributed governance consists of international and national regulations, legislation, standards, and contractual agreements among organizations and institutions that enable the smooth operation and expansions of all that infrastructure. Moreover, governance enables the emergence of public and commercial activities through, for instance, the acknowledgement of domain names, copyright, tax payment and electronic signatures. Finally, it aims at preventing misuse of internet by, e.g., detection of criminal activities.

All these public values hold equally for a quantum version of the internet. To maintain them new governance mechanisms will have to be developed, for the phase in which the quantum internet gets introduced, and for the phase in which it is more established. This is because quantum internet will substantially change the way we can communicate. For example, it makes available new encryption methods of that communication, which may require new governance for surveilling that communication to maintain security. The future use of quantum internet may, furthermore, reveal that new public values have to be protected, requiring new forms of governance. For example, twenty years ago we probably did not imagine that the usage of classical internet can lead to substantial privacy infringements. Hence privacy emerged through the usage of classical internet as a value for which new governance was needed. New surprises are to be expected once the quantum internet will be used on a regular basis.

Co-evolution of quantum internet and its governance



During the introductory phase equal access may be an issue

Let's explore a little bit more the values for which governance of the quantum internet may be needed. In the phase in which the quantum internet is introduced, issues emerge about values such as security, privacy, flexibility, trust and equal access. Initially, the quantum internet will be available to a few pioneering users in academia and industry, and a value issue that then emerges is one of equal access. Do we want it to develop to a public infrastructure? If we want this, regulation and legislation can direct the development of quantum internet in this direction.

Quantum computing raises additional issues

Looking beyond quantum internet, the emergence of quantum computing raises issues of security, privacy and trust. Quantum computing may make current encryption of communication vulnerable, enabling users of quantum computers to infringe on the privacy of others. Digital databases containing state or industrial secrets can be decrypted, leading to security issues. Moreover, daily communication that uses security, such as financial transactions, video links, GPS signals and software updates, may be decrypted leading to real or perceived breaches in public trust in these vital forms of communication. Governance may be the response to these threats. It may be necessary to install legislation that requires better encryption of databases or to regulate the use of quantum computers by private parties. It may also lead to policies speeding up the development and use of quantum internet for securing financial transactions, GPS signals and software updates. The quantum internet may thus actually restore public values such as security, privacy and trust in communication. Yet, to be able to play this role governance needs to be in place first. Users from banks to governmental agencies may decide to use the quantum internet for securing their communication only when quantum internet encryption tools are standardized and certified.

Governance can protect and promote values

Once the quantum internet is established and all its users can engage in secure communication, a security issue surfaces about surveillance. Possibilities for scanning digital communication for its content, for policing or for national security reasons, become limited. Governance may mean that only those quantum internet encryption tools will be allowed that enable states to decrypt it, say through a security backdoor or through other measures. The question is whether this is desirable, since others might use the backdoor as well, and – again – governance will be needed to regulate the use of such decryption capabilities. Governance is, however, not just a response when public values are jeopardized; it also enables the realization of such values. It may create trust in the use of the quantum internet and it may through that trust, foster economic growth by offering companies a basis to develop new activities and opening up new markets. That new commercial development may, like the classical internet, raise new issues about public values. And it is again governance that is to direct the usages and developments towards avoiding undesired effects.

Waiting too long poses a risk

To be able to judge which regulations, legislation and institutions are needed, governing organizations, from states to banks, should inform themselves about what the quantum internet may bring. The outcome may be that it brings gradual changes, implying that changes in governance can be gradual as well. However, a serious risk is that governance is initiated too late, as for instance regulation for data protection only emerged after privacy was violated for a while. More knowledge about this impact may also lead to the conclusion that immediate action is needed for bringing the innovation the quantum internet brings in sync with our public values.

The impact of quantum technologies on the payment system

An interview with Oscar Covers

Cybersecurity Analist at the Dutch Payments Association

What are the main tasks of the Dutch Payments Association?

The Dutch Payments Association cooperates with its members towards safe, efficient, reliable and accessible payments in the Netherlands. Our members provide regulated payment services: banks and payment institutions. Among others we cooperate to keep electronic payments safe and to prevent fraud. We also assist with setting reliable standards.

What is your job at the Dutch Payments Association?

In the Netherlands we have a common understanding that competition on security makes no sense. Consequently the financial sector works closely together to keep financial services safe and secure, in the Netherlands as well as internationally.

As a cyber security analyst, I interpret internet or cyber threats, together with the experts of financial institutions. We make risk assessments and we look for risk mitigating measures. We share best practices and each member can choose the measures that are most effective for their own organization. In short, I analyze, anticipate and consult.

TU Delft is working on quantum internet and quantum computing. These technologies are expected to have an impact on the security of communication, including the security of electronic payments. Quantum computing may enable breaking encryption of such communication, and quantum internet offers new encryption through quantum key distribution. How realistic are these expectations?

At the end of 2015 we first heard about the developments, opportunities and threats related to quantum computing. Mature quantum computers can be expected by 2030 and we should start to prepare. The Dutch Payments Association has already organized four expert sessions with participants from universities, banks and payment companies and experts in the field of quantum and crypto.

These sessions taught us that the computing power of existing quantum computers is still very limited. Nevertheless, two known quantum algorithms pose a threat to a number of widely used encryption algorithms, if implemented on future powerful quantum computers.

We expect the first practical quantum computers to be deployed in the chemical and medical industries. These applications provide an early warning because to break current encryption algorithms, still more quantum computing power will be needed.

Our approach is to define 'low regret moves': steps we can take now without regretting them later on. Quantum key distribution will assure secure communication in a quantum computer era but the solution must also fit economically with business processes. In addition, it is preferable to introduce modifications through regular replacement, as accelerated replacement incurs more expenses.

How is the Dutch Payments Association preparing for the possible impact of quantum technologies on the security of electronic payments?

On a regular basis we will validate the previously defined 'low regret moves' and update them if necessary. Examples of these low regret moves are:

- Developing scenarios;
- Selecting encryption systems that are safe in a quantum computer era, known as 'post-quantum crypto';
- Gaining experience, for example by implementing post-quantum crypto systems.

This year we decided to make a readiness inventory, listing all the business processes that use encryption. For each business process the encryption algorithm and key length are then specified. We also determine the shelf life and enumerate which post-quantum crypto alternatives are available. Finally we try to set a realistic migration period. How much time does it take to migrate from the current situation to the situation that the business process uses post-quantum crypto?

What can TU Delft offer to the Dutch Payments Association to anticipate the impact of quantum technology?

We would like TU Delft to participate in our regular expert sessions in which we update low regret moves and, if possible, add new ones. In the field of post-quantum cryptography a lot of fundamental research is still being carried out and we have to start thinking about the implementation. We can use some help with that.

We also want to gain experience on a testing environment, when implementing post-quantum cryptography. In order to make optimal use of post-quantum cryptography, current protocols will most likely have to be redesigned. We already know that simply replacing algorithms will lead to very inefficient processes. So again, we can use your help.

Moving towards quantum resilience

An interview with Jaya Baloo

Chief Information Security Officer at KPN

What triggered your interest in quantum communication?

My interest in quantum communication arose more than a decade ago when I was working on lawful interception and we discussed how we could accomplish lawful interception in the face of quantum communication. It really opened up my eyes to the possibilities of how we could guarantee security in the face of all types of monitoring threats. When things are encrypted mathematically, there might be a backdoor that we don't know about or there might be threats that we haven't fully understood. But with quantum, it's encrypted at the physical layer. That is a totally different ballgame.

Where do you see the opportunities for a company like KPN?

We are only at the beginning of what quantum communications could mean for our society, certainly in terms of ubiquitous usage. Today, we mostly talk about point-to-point links. But it only becomes powerful when you can communicate many to many, on demand, instantly. This is the goal of projects that are being done now, creating quantum repeaters and architecture building blocks for a new type of quantum communications-delivered internet. I consider this to be the most exciting thing that will happen in the next few years. KPN would like to be one of the first providing such a network.

What do you recommend to companies that aim to become quantum resilient?

The idea of quantum resilience is that regardless of whatever happens, even with a quantum computing attack, your communications remain secure. I recommend a 3-step plan towards quantum resilience:

1) Buy yourself some time. Assess the cryptography you currently use, and what you use it for. Make sure that you're using the maximum key length option for your current cryptography. Assess the cryptographic agility you have with your current cryptographic algorithms, in other words, your capacity to adopt other encryption methods without significant changes to your system infrastructure.
2) Look for specific places in your network where quantum key distribution would be an asset. For example, primary and secondary data center connections or crucial places for particular transactions that are mission-critical. Those areas will need to be planned for and examined, and built out. The technology is available today off the shelf, so there should really be no reason to not do it for a few places, but this does not scale well across large distances or networks.
3) Think about how you can fully explore crypto agility by replacing current algorithms with post-quantum cryptography. This is a new set of post- quantum algorithms that are currently under submission for NIST, but you can already start playing around with them now. There are different cryptographic algorithms, each with a specific purpose and yet different merits. You can already start examining, especially for critical data, which one works the best for you. This way you learn if it's possible to, and how easy it is to, swap one algorithm for another. It is all about crypto agility. We use different cryptographic algorithms for our internet connections than for our VPNs or for our banking algorithms. I recommend that regardless of what industry you're in, you examine how you use cryptography today and which algorithms you use for that, and then take a look at the best possible post-quantum mix for your future business.

Why did KPN choose to partner with TU Delft in building a quantum internet?

The partnership with TU Delft gives us an advantage to be better prepared for the future by participating in the present. We will be better able to cope with new technologies if we're part of the build and development, compared to being only part of the group that needs to adopt and follow once it's there. Finally, it's an honor to be part of such inspirational endeavors with a partner that does such groundbreaking work on all things quantum.

When do you expect a commercial quantum network service?

Initial forays to provide quantum computing services are already being commercialized now, and we'll see several providers doing that. For quantum communication, there is quite a bit of work being done by different companies on quantum key distribution and hardware, but it's not being deployed as a managed service yet. We will first see managed services for point-to-point links that will provide quantum-grade security. When we can extend this to entire network services, it becomes really interesting. But a lot of fundamental research still needs to happen. Developing a quantum repeater is not a small task, as it is not just the technical challenges, it's also making sure there is funding and the cooperation of all parties that are necessary to make this a success. We'll count ourselves fortunate if we'll see a commercially available quantum internet in the next five to ten years.

Bridging expertise in quantum and classical networks

An interview with Daniel Karrenberg

Chief Scientist at RIPE NCC

What is RIPE NCC's role in the development of quantum networks?

The RIPE NCC is an independent association of classical internet providers. We support the infrastructure of the internet through technical coordination. We're also an open space for exchanging ideas on, for example, quantum networks. Everyone in the space of classical networks should understand what's coming, specifically in the area of cryptography, because the best-before date on the encryption we're using today is rapidly diminishing.

You are a true internet pioneer. How do you see your own role in the development of quantum networks?

I want to help connect the quantum networking work with the classical protocol work, and I'm focusing on making the right connections to get it going. In practice, the people who know a lot about protocols have little knowledge of quantum networks. And the people working on quantum networking usually don't know much about protocols. They need to have enough understanding of each other's spheres in order to have a successful interdisciplinary collaboration.

What can we learn from the development of the classical internet?

Conceptually, I would like to see an architecture that can grow organically without central coordination or supervision – as is the case with the classical internet. How can we apply the same design principles in building a quantum internet, allowing decentralised growth by allowing local interconnections?

How important are open standards and what are the challenges involved to make it happen?

We need to work on open standards for a quantum internet from the start. In the classical internet, it's a mixed bag; even today we struggle in some areas with intellectual property rights which sometimes hinders interoperating.
In my opinion, universities could have a bigger economic and societal impact if they could find ways for researchers in academia to get credits for the efforts they spend in developing – or help developing – open protocol specifications in an interdisciplinary way. Today, researchers are for a large part evaluated based on publications. And an open protocol standard doesn't count as a 'real' publication.

What is the potential effect of big tech companies' involvement in the early development stages of quantum networks?

It is no surprise that big tech companies are taking a big role; you need serious amounts of money to equip labs. You can't do it in a garage, which makes it very different from the development of the classical internet. But who knows, someone might come up with a radically different way to create stable qubits that doesn't require expensive equipment, and suddenly we'll see an explosion of developments.
The trend that I've seen emerge over the past five years in the classical networking space is that even the most closed big tech companies are now realising that there's an advantage to sharing the basic technology in open source communities. They won't make it available in a productised version, but they will make some of the basic underlying foundations available for those who know where to look. This fosters spin-off developments and applications of that basic technology that they couldn't develop themselves because money just can't buy that. You need to engage the right minds. They can find ways to monetise it later on, and also use the open source community for recruitment purposes. IBM is moving a little bit in this direction with their publicly available quantum computer in the cloud.

Who will be early adopters?

Governments and other companies and institutions that need strong encryption today. Quantum key distribution is the first powerful use case. The promise of the quantum internet is that it will make it feasible to share one-time pads between anyone who needs strong encryption. In the beginning, this will still be quite expensive, but I hope that it will become affordable and available even to individuals like you and me before our current crypto becomes too vulnerable.

Do you see any dangers in blind quantum computing?

The concept is fascinating. In practice, I don't think it is that different from what you can do right now. If money is no object, you can harness diverse cloud computing resources on a massive scale, and thereby obfuscate what you are really computing quite well.

When should regulation come into play?

It's much too early for governments to think about regulation. Governments are just finding their way in governing the internet, finding the right balance between regulating and not-regulating the internet. The quantum internet doesn't even exist. Thinking about the possible impact is a good thing, but regulation is two steps further. It's very useful that TU Delft is also taking up a role on thinking about the impact of quantum technology.

Reflection

A Quantum Technology Revolution and an Evolution

From a technological point of view a revolution is taking shape. Ground-breaking research on quantum technology is being done at TU Delft and at institutions all over the world. A whole new kind of physics is made available to communication and computation. Quantum theory has been applied since the technology of, say, transistors, and laser is also based on quantum theory. Yet quantum internet and quantum computers introduce superposition and entanglement as central means for communication and computation. And that is truly new. Quantum technology creates a revolution by offering all kinds of new applications within communication, computation, sensing, etc. These new applications are game changers that could have a disrupting impact on society.

However, our exploration yielded that the introduction of quantum technology shows similarities with the impact of other (new) technologies. Rather than a revolution, the advent of quantum technology will gradually change and improve existing applications. The impact of these new applications in the domain of communication technology is not necessarily seen by stakeholders as revolutionary or game-changing, but it is assessed as highly impactful. So, from a societal point of view, quantum technology will be evolutionary rather than disruptive. This evolutionary perspective is more productive when considering the possible impact of quantum internet.

Communication security

Take security of communication, for example. If quantum computers become available, the most widely used encryption methods for securing communication can be cracked. Were this to be a sudden event, the cracking would lead to a security crisis in communication. Messages sent over the internet, from email to data transfer become transparent to third parties, which in turn may compromise the global financial system. To curb this crisis, an urgent call to action will be required. Post-quantum encryption methods that withstand quantum computing should be swiftly put in place: telecom corporations, banks and other institutions should immediately migrate to these new post-quantum encryption methods. At the same time, we should speed up realizing a quantum internet that enables fully secure encryption through quantum key distribution.

Seen from the evolutionary perspective, some of the post-quantum encryption methods are already available and banks are already regularly updating their encryption policies in response to new security threats. A smoother response to the impact of quantum computers can then be envisioned: telecom corporations, banks and institutions can (and should) start to include post-quantum encryption methods in their security updates. This smoother response can be enabled by making information available about the emergence of quantum technologies and by giving estimates when existing encryption methods may become vulnerable to quantum computing.

At TU Delft we see it as our societal responsibility to give industry and society at large information about quantum technologies and their possible impact. We are ready to help stakeholders with building up a knowledge base to arrive at an independent and balanced evaluation of how to respond to the new applications of quantum technology. And we see our efforts to build a quantum internet as our contribution to add new means for communication security. This creation of the quantum internet will moreover not be enough. For building up trust in the use of quantum internet for encrypting communication, we will also support efforts towards certification of this encryption.

Access to quantum internet

A second topic that we encountered in our exploration is that of the accessibility of quantum internet to users. Research and development of quantum technologies are currently taking place in academic institutions and the high-tech industry, regularly in productive collaboration, as is also done at TU Delft. Seen from a revolutionary game-changer perspective, this may bring about a situation in which quantum technology is primarily owned and operated by a few large commercial companies. This may lead to commercial monopolies of the applications of quantum technology, or more mildly to conflicts of interests between companies and other users.

However, for arriving at a global quantum internet, an evolutionary perspective is probably more appropriate. Like with the classical internet, the quantum internet will gradually grow and no single entity will 'own' the quantum internet. Instead, it will be a network of connected quantum systems, all working with the same set of protocols. It will need infrastructure and quantum network devices, which will be owned, managed and supervised by many different – commercial and non-commercial – parties. As is the case with the classical internet today.

At TU Delft we aim at making quantum technology accessible to all. We, for instance, contribute to a public quantum internet through our efforts in the Quantum Internet Alliance and quantum internet hackathons. Together with partners we strive to design scalable quantum networks and pursue a quantum internet that is available to all.

Cyber security

These two topics combined – access to quantum internet and communication security – bring us to national issues of cyber security in law enforcement and defence. Quantum internet with its encryption capabilities gives a clear advantage to those parties that have it first: these early adopters can then shield their communication from others. And quantum computing with its decryption capabilities, gives a clear advantage to those parties that can do it first, for those early adopters can start reading communication and decrypting state and industrial secrets. From the revolutionary perspective, you would then expect major disruptions of security and military balances, say when some actors – states or companies – start decrypting the secrets of others, or when communication by some actors – criminal or not – cannot be intercepted anymore by police forces.

From the evolutionary perspective balances will get disturbed, but will eventually reach a new – perhaps slightly different – balance. Law enforcement has to change its methods of intercepting communication, for instance by focussing more on the front and back end of communication. It may also benefit from better encryption of its own communication. The evolutionary perspective will not completely rule out disruptions between actors and states: you can envision new waves of information becoming public, as occurred around WikiLeaks and the Panama Papers. And you can expect a quantum technology version of the current power struggles in cyber space. The evolutionary perspective points, however, at the importance of building up the knowledge base about quantum technology quickly, also at the level of governments.

At TU Delft we aim to make this knowledge available for giving stakeholders the means to anticipate possible disruptions in cyber security, and for enabling that all can benefit from the new applications that quantum technology can bring to society.

Pieter Vermaas, chair

Deborah Nas

Lieven Vandersypen

David Elkouss

Special thanks

This magazine is the result of a joint effort of the quantum vision team and all the experts with whom we have spoken to understand what quantum internet is about and what its impact on society and industry can be.

The vision team was installed by the Executive Board of TU Delft. We want to thank Tim van der Hagen, Rector Magnificus and President of the Executive Board, for his vision and trust in the effort, and Jeroen van den Hoven, University Professor at the faculty of Technology, Policy and Management, for his initiation role. We acknowledge Ronald Hanson, Scientific Director of QuTech, and Stephanie Wehner, Roadmap Leader Quantum Internet and Networked Computing, for their help, and the vision team members for their work.

We organized five workshops with science journalists, innovators and designers, industry, law enforcement and defence, and governmental organisations. We are grateful for the input from all of these experts from inside and outside of TU Delft, and we heartily thank all workshop participants for their commitment and challenging contributions.

A special mention goes to the students of TU Delft who participated in the vision team. Aletta Meinsma and Willem Evers not only created much content, but also proposed the format of a magazine to present the results of the effort, which was designed by Júlia Fort Muñoz.

Pieter Vermaas, chair
Deborah Nas
Lieven Vandersypen
David Elkouss Coronas

Lotte Asveld,
Assistant Professor,
Faculty of Applied Sciences

Julia Cramer,
Outreach Coordinator QuTech,
Faculty of Applied Science

Slava Dobrovitski,
Group Leader QuTech,
Faculty of Applied Sciences

David Elkouss Coronas,
Scientific Researcher QuTech,
Faculty of Electrical Engineering, Mathematics and Computer Science

Willem Evers,
Student,
Faculty of Industrial Design Engineering

Marijn Janssen,
Full Professor,
Faculty of Technology, Policy and Management

Júlia Fort Muñoz,
Student,
Faculty of Industrial Design Engineering

Deborah Nas,
Full Professor,
Faculty of Industrial Design Engineering

Aletta Meinsma,
Student,
Faculty of Applied Sciences

Gary Steele,
Full Professor,
Faculty of Applied Sciences

Tim Taminiau,
Group Leader QuTech,
Faculty of Applied Sciences

Lieven Vandersypen,
Roadmap Leader QuTech,
Full Professor,
Faculty of Applied Sciences

Pieter Vermaas, chair
Associate Professor,
Faculty of Technology, Policy and Management

Richard Versluis,
Systems Engineer QuTech,
TNO

Kees Vuik,
Full Professor,
Faculty of Electrical Engineering, Mathematics and Computer Science

For contacting us:

Leonie Hussaarts
Manager Communication

TU Delft / Faculty of
Applied Sciences - QuTech

T +31 (0)6 38 67 84 19
E l.hussaarts@tudelft.nl
www.qutech.nl

Workshop participants

Michel van Baal (TU Delft)

Frank Bekkers (The Hague Centre for Strategic Studies)

Ed van Brecht (TNO)

Gabriele Bulgarini (Single Quantum)

Rob Christiaanse (Efco Solutions)

Oscar Covers (Betaalvereniging Nederland)

Patrick van der Duin (Stichting Toekomstbeeld der Techniek)

Martijn Egberts (Landelijk Parket, OM)

Jeroen van Erp (TU Delft)

Dimitri van Esch (ABN Amro)

Laurens Gaukema (NOS Tech)

Patrick de Graaf (TNO)

Ferdinand Griesdoorn (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties)

Freeke Heijman (Ministerie van Economische Zaken en Klimaat en Nationale Wetenschapsagenda)

Paul Hekkert (TU Delft)

Kevin van Hoogdalem (Microsoft)

Tomasz Jaskiewicz (TU Delft)

Frederick Kerling (Atos)

Dennis Kersten (Accenture)

Maaike Kleinsman (TU Delft)

Gerd Kortuem (TU Delft)

David de Nood (VNO-NCW)

Corsin Pfister (KPN)

Charlotte Rugers (Ministerie van Defensie)

Maarten van der Sanden (TU Delft)

Wouter Smit (Belastingdienst)

Marlies Struyvé (Ministerie van Economische Zaken en Klimaat)

Jolien Ubacht (TU Delft)

Joost van der Vleuten (Ministerie van Economische Zaken en Klimaat)

Bruno van Wayenburg (NRC Handelsblad)

Rene Wiegers (NLR – Netherlands Aerospace Centre)

References

General references

QuTech
QuTech is the advanced research center for Quantum Computing and Quantum Internet, a collaboration founded in 2014 by TU Delft and the Netherlands Organisation for Applied Scientific Research (TNO).
www.qutech.nl

QuTech Academy
To build the first quantum computer and quantum internet, QuTech works together with talented students with in-depth knowledge in the areas of both quantum physics and computer science & engineering.
www.qutech.nl/academy

Quantum Manifesto
A New Era of Technology
A call to the Member States of the European Union and to the European Commission to launch a €1 billion flagship-scale initiative in Quantum Technology, 2016
https://qt.eu/app/uploads/2018/04/93056_Quantum-Manifesto_WEB.pdf

The Quantum Flagship
The site of the European Union's large scale research program on quantum technologies. It will spend over 10 years an amount of 1 billion Euro on research and development.
www.qt.eu

Quantum Internet Alliance
The site of the Quantum Internet Alliance, proving information about the European ambition to build a Quantum Internet that enables quantum communication applications between any two points on Earth
www.quantum-internet.team

The Societal Impact of the Emerging Quantum Technologies
A special issue of the journal Ethics and Information Technology with contributions from scholars in quantum technology, technology assessment and philosophy.
Edited by Pieter Vermaas, Delft University of Technology, 2017.
https://link.springer.com/journal/10676/19/4/page/1

The UK National Quantum Technologies Programme
A site containing various reports and resources about quantum technologies as part of the United Kingdom efforts on quantum technologies.
http://uknqt.epsrc.ac.uk

Quantum Computing: Progress and Prospects
An extensive introduction that focusses on the technology of quantum computing, and "assesses the feasibility and implications of creating a functional quantum computer capable of addressing real-world problems".
Edited by Emily Grumbling and Mark Horowitz, National Academies of Sciences, Engineering, and Medicine.
The National Academies Press, Washington, DC, 2018.
www.nap.edu/catalog/25196/quantum-computing-progress-and-prospects

The Next Decade in Quantum Computing – and How to Play
The Next Decade in Quantum Computing – and How to Play
A report on the development of quantum computing in the next five to ten years, focussing on the technology, the applications and the main players.
By Philipp Gerbert and Frank Ruess, Boston Consultancy Group, 2018.
http://image-src.bcg.com/Images/BCG-The-Next-Decade-in-Quantum-Computing-Nov-2018-21-R_tcm9-207859.pdf

Other references

Page 8-9. Quantum mechanincs and quantum technology 1.0
www.en.wikipedia.org/wiki/Introduction_to_quantum_mechanics

https://commons.wikimedia.org/wiki/File:Solvay_conference_1927.jpg

www.tudelft.nl/en/2018/tu-delft/exhibition-the-age-of-standards/

Pages 10-11. Quantum technology 2.0
The High-Level Steering Committee, "Quantum Technologies Flagship Final Report," June 2017.
https://ec.europa.eu/digital-single-market/en/news/quantum-flagship-high-level-expert-group-publishes-final-report

Pages 14-15. Classical internet and quantum internet
www.dictionary.com/browse/internet

www.unit-conversion.info/texttools/convert-text-to-binary/

www.history.com/topics/inventions/invention-of-the-internet

www.quantum-internet.team/

Pages 16-17. Public key cryptography and quantum key distribution

www.csrc.nist.gov/projects/cryptographic-standards-and-guidelines/archived-crypto-projects/aes-development

Kaliski, B. The Mathematics of the RSA Public-Key Cryptosystem. RSA Laboratories.

Mosca, M. (2016). A quantum of prevention for our cyber-security. Institute for Quantum Computing & Special Advisor on Cyber Security to the Global Risk Institute, Toronto
NIST. (2017). Post-Quantum Cryptography. Project Overview.

Pages 18-21. Quantum networks

S. Wehner, D. Elkouss, and R. Hanson, "Quantum internet: A vision for the road ahead," Science, vol. 362, no. 6412, 2018.

Hensen and et al, "Loophole-free bell inequality violation using electron spins separated by 1.3 kilometers," Nature, vol. 526, no. 628, 2015.

www.phys.org/news/2018-01-real-world-intercontinental-quantum-enabled-micius.html

https://www.sciencemag.org/news/2017/06/china-s-quantum-satellite-achieves-spooky-action-record-distance

Pages 22-23. Quantum computing

Picture: Copyright Marieke de Lorijn

Pages 24-25. Quantum repeaters and quantum teleportation

Sangouard, N. et al. (2011). Quantum repeaters based on atomic ensembles and linear optics. Rev. Mod. Phys. 83, 33-80.

Pages 32-33. Secure communication

www.newscientist.com/article/dn12786-quantum-cryptography-to-protect-swiss-election/

KPN (2016). KPN to implement quantum encrypted connection (QKD).

Pages 34-35. Secure login in networks

I. Damgård, S. Fehr, L. Salvail, C. Schaffner, Secure identification and QKD in the bounded-quantum-storage model. Theor. Comput. Sci. 560, 12 (2014). doi: 10.1016/j.tcs.2014.09.014

F. Dupuis, O. Fawzi, S. Wehner, Entanglement sampling and applications. IEEE Trans. Inf. Theory 61, 1093–1112 (2014). doi: 10.1109/TIT.2014.2371464

Pages 36-37. Various other applications

https://journals.aps.org/prx/abstract/10.1103/PhysRevX.4.021047

Pages 38-39. Quantum enhanced GPS

www.gps.gov/systems/gps/performance/accuracy

“It’s very useful that TU Delft is also taking up a role on thinking about the impact of quantum technology”

Daniel Karrenberg - RIPE NCC

“We are only at the beginning of what quantum communications could mean for our society, certainly in terms of ubiquitous usage”

Jaya Baloo - KPN

“People need to be able to interact with a quantum internet, and play around with it to develop new applications. I’m sure that the technology will spark off innovations, but we don’t know yet what they will be”

Stephanie Wehner - TU Delft

“Quantum key distribution will assure secure communication in a quantum computer era, but the solution must also fit economically with business processes”

Oscar Govers - Dutch Payments Association

Let's explore the future of the quantum internet together

The quantum vision team

Quantum internet

The internet's next big step

QUANTUM VISION TEAM

TU Delft